DIRECTORY

GO

C Intranet ◉ Directory

NEWS
Executive Briefings
Intelligence Reports
Division Newsletter
Announcements
Calendar

ABOUT US
Organizational Chart
Collateral Duties and Program Representatives
Directory
Evacuation Plan

ORGANIZATION
Front Office
Computer Intrusion Section (CIS)
Cyber Crime Section (CCS)
Information Sharing & Analysis Section (ISAS)

RESOURCES
Applications
Forms
Training
Policy
Library
Downloads
FAQs
Useful Sites

ISAS: Public Private Alliance Unit (PPAU)

InfraGard Information:

History

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI sponsored program, and will work with DHS in support of its CIP mission, facilitate InfraGard's continuing role in CIP activities, and further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

Front Office - Room 5842

[redacted]
Unit Chief
[redacted]
Fax:
[redacted]

b6
b7C

About Us

Office Assignments
InfraGard Secure Web Site
Additional InfraGard Information
Staff Directory

Resources

2007 InfraGard Conference Presentations
All Field Office ECs
Chapter News & Updates
Document & Forms
PPAU News & Links
Unit Calendar
Unit Presentations

b7E

[redacted]

[redacted] LA) (FBI)

From: [redacted] (OGC) (FBI)
Sent: Thursday, July 12, 2007 1:01 PM
To: [redacted] (LA) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI); [redacted] (CyD) (FBI)
Cc: [redacted] (OGC) (FBI); [redacted] (CyD) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

b6
b7C

UNCLASSIFIED
NON-RECORD

THIS DOCUMENT IS A PRIVILEGED FBI ATTORNEY COMMUNICATION AND MAY NOT BE DISSEMINATED WITHOUT OGC APPROVAL

[redacted] Thanks for the input.

[redacted] Please review our Civil Litigation Unit's analysis and concerns (below) -- and discuss with NH and your superiors. If you choose to [redacted] please provide me (OGC) with a draft.

b5
b6
b7C

[redacted]
Assistant General Counsel
Science & Technology Law Unit
Office of the General Counsel
[redacted] JEH Room 5965

THIS IS A PRIVILEGED COMMUNICATION AND IS NOT TO BE FURTHER DISSEMINATED WITHOUT PRIOR OGC APPROVAL.

-----Original Message-----
From: [redacted] (LA) (FBI)
Sent: Wednesday, July 11, 2007 12:33 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

b6
b7C

UNCLASSIFIED
NON-RECORD

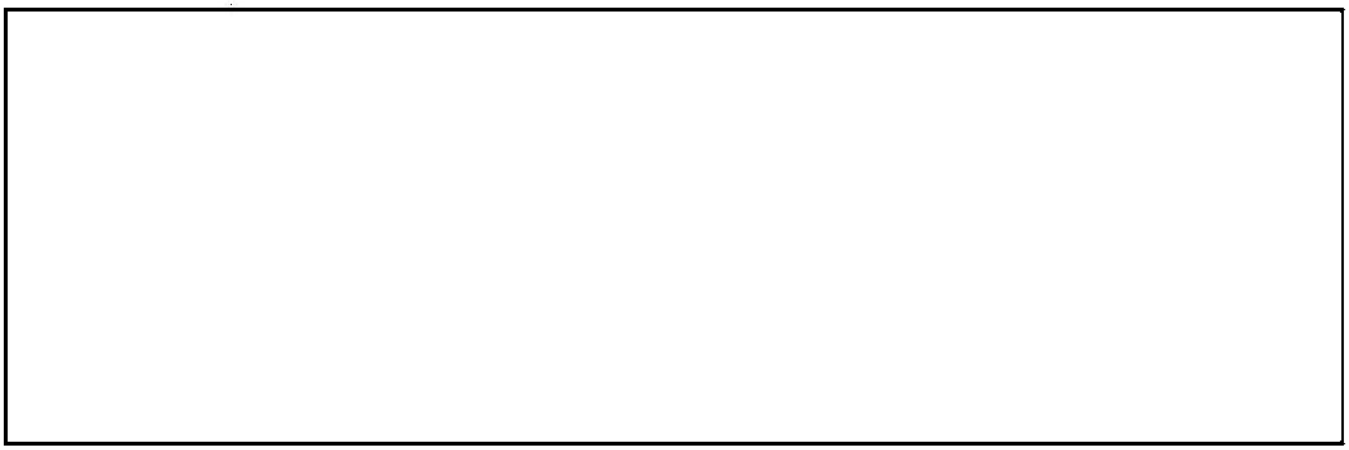
[redacted] - As I understand it from the email, [redacted]

[redacted] The proposal is to [redacted]

b5
b6
b7C

[redacted]

b5



b5
b6
b7C

I hope this helps - let me know if you need anything else.

b6
b7C

THIS DOCUMENT IS A PRIVILEGED FBI ATTORNEY COMMUNICATION AND MAY NOT BE DISSEMINATED WITHOUT OGC APPROVAL

-----Original Message-----
From: (OGC) (FBI)
Sent: Wednesday, July 11, 2007 6:58 AM
To: (LA) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

b6
b7C

UNCLASSIFIED
NON-RECORD

Anything on this. The Infragard folks are still waiting for an answer. Do you need more info? If so, what?

b6
b7C

Please advise.

Thanks,

-----Original Message-----
From: (OGC) (FBI)
Sent: Monday, July 02, 2007 3:57 PM
To: (LA) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

b6
b7C

UNCLASSIFIED
NON-RECORD

b6
b7C

INMA is the Infragard National Membership Alliance. It is a non-profit organization that runs the National Infragard chapter, which sets agendas for the local chapters (at the FO level). It is basically a public-private information sharing network with a vetted membership that was started by the FBI.

Check this out:

b7E

If you need more info, please let me know.

Thanks,

[redacted]-Original Message-----
From: [redacted](LA) (FBI)
Sent: Thursday, June 28, 2007 5:38 PM
To: [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] can you tell me more about what the IMA is and what it does?

thanks

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Thursday, June 28, 2007 2:35 PM
To: [redacted](OGC) (FBI)
Cc: [redacted](LA) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

THIS DOCUMENT IS A PRIVILEGED FBI ATTORNEY COMMUNICATION AND MAY NOT BE DISSEMINATED WITHOUT OGC APPROVAL

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]
We will need some more info before giving you advice. It is assigned to [redacted] Please send the info to him. Sorry for the delay. Thanks,
[redacted]

b6
b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Wednesday, June 20, 2007 7:30 AM
To: [redacted](OGC) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

UNCLASSIFIED
NON-RECORD

[redacted]
Any word on this issue re: [redacted]

Please advise.

Thanks,

b5
b6
b7C

[redacted]

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Monday, June 11, 2007 1:29 PM
To: [redacted](OGC) (FBI)
Subject: FW: NH INFRAGARD IMA ISSUES

b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]
I got the questions below. ALU is working the second one. As for the first issue, from a CLU perspective [redacted]

b5
b6
b7C

[redacted] b5

Please advise when you get a chance.

Thanks,

[redacted]

[redacted] A PRIVILEGED FBI ATTORNEY [redacted]
AND MAY NOT BE DISSEMINATED WITHOUT OGC APPROVAL

-----Original Message-----
From: [redacted] (CyD) (FBI) b6
Sent: Sunday, June 03, 2007 4:26 PM
To: [redacted] (CyD) (FBI); [redacted] (CyD) (FBI) b7C
Cc: [redacted] (CyD) (FBI); [redacted] (OGC) (FBI)
Subject: RE: NH INFRAGARD IMA ISSUES

UNCLASSIFIED
NON-RECORD

Please refer these questions to AGC [redacted] since they are legal in nature.

As to the first question [redacted] b5
b6
b7C

As for the second question [redacted]

[redacted]

-----Original Message-----
From: [redacted] (CyD) (FBI)
Sent: Thursday, May 10, 2007 5:23 PM
To: [redacted] (CyD) (FBI); [redacted] (CyD) (FBI) b6
Cc: [redacted] (CyD) (FBI) b7C
Subject: FW: NH INFRAGARD IMA ISSUES

UNCLASSIFIED
NON-RECORD

[redacted]

[redacted] called today in reference to the question below and I deferred an answer to you gentlemen You're thoughts on [redacted] See below. b5
b6
b7C

Have a good week.

SSA [redacted]

-----Original Message-----
From: [redacted] (NH) (FBI)
Sent: Thursday, May 10, 2007 4:35 PM
To: [redacted] (CyD) (FBI) b6
Cc: [redacted] (NH) (FBI) b7C
Subject: NH INFRAGARD IMA ISSUES

UNCLASSIFIED
NON-RECORD

[redacted] b6
b7C

Per our conversation, yesterday (May 9) was our quarterly IMA meeting which was attended by 84 members. The program was a table top exercise run by the FBI and USCG regarding a terrorist attack on transportation hubs (similar to Mumbai and London - trains and buses) and the issues related to business continuity of operations. The program was very well received. After the members meeting the IMA Board of Directors monthly meeting was held. Two issues were raised by the BOD requesting FBI guidance/assistance.

[redacted] b5

Thanks

[redacted]
NH InfraGard Coordinator

[redacted] b6 b7C

THIS DOCUMENT IS A PRIVILEGED FBI ATTORNE[illegible]
AND MAY NOT BE DISSEMINATED WITHO[illegible]

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION
FOI/PA
DELETED PAGE INFORMATION SHEET
FOI/PA# 1643419-000

Total Deleted Page(s) = 8
Page 13 ~ b5;
Page 14 ~ b5;
Page 15 ~ b5;
Page 16 ~ b5;
Page 17 ~ b5;
Page 18 ~ b5; b6; b7C; b7E;
Page 19 ~ b5;
Page 20 ~ b5;

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

State of Delaware
Secretary of State
Division of Corporations
Delivered 11:30 AM 09/09/2004
FILED 11:30 AM 09/09/2004
SRV 040654327 - 3645152 FILE

CERTIFICATE OF AMENDMENT TO THE CERTIFICATE OF INCORPORATION OF INFRAGARD, INC.

Infragard, Inc., a corporation organized and existing under and by virtue of the Delaware General Corporation Law (the "Corporation"), does hereby certify:

FIRST: That on June 29, 2004, the Board of Directors of the Corporation adopted a resolution setting forth proposed amendments to the Certificate of Incorporation of the Corporation, declaring said amendments to be advisable and submitting the proposed amendments to the local chapters of the Corporation for their consideration and approval, such proposed amendments being as follows:

To delete Article FIRST of the Corporation's Certificate of Incorporation in its entirety and substitute in its place a new Article FIRST to read as follows:

> "**FIRST:** The name of the corporation (hereinafter called the 'Corporation') shall be Infragard National Members Alliance, Inc.";

To delete Article THIRD of the Corporation's Certificate of Incorporation in its entirety and substitute in its place a new Article THIRD to read as follows:

> "**THIRD:** The Corporation shall be authorized and empowered to pay reasonable compensation for services rendered and to make payments and distributions in furtherance of the purposes set forth in Article SECOND hereof.";

To delete Article FIFTH of the Corporation's Certificate of Incorporation in its entirety and substitute in its place a new Article FIFTH to read as follows:

> "**FIFTH:** to further the Corporation's objects and purposes, the Corporation shall have and shall exercise all the powers conferred by the provisions of the laws of the State of Delaware upon nonstock corporations that are consistent with the scope of Article SECOND hereof. Without limiting the generality of the foregoing, the Corporation shall have the power to sue and be sued, to own, to take title to, receive and hold, lease, sell and resell, in fee simple or otherwise, property, real, personal or mixed, wherever situated or however acquired, without limitation as to amount or value. The Corporation shall have the right, power and authority: to receive gifts, bequests and contributions outright, in trust or in any other form; to grant and exercise options to buy or sell; to encumber property by deed of trust, pledge or otherwise; to borrow money and secure payment of same by placing one or more liens on the realty

and/or personal property of the Corporation; to lease, build, or erect, remodel, repair, construct and/or reconstruct any and all buildings, houses, or other structures necessary, proper or incident to the carrying out of the objects and purposes stated herein. The Corporation shall have the right, power and authority to collect dues, and to use, apply, invest and reinvest the principal and/or income therefrom or to distribute the same for the purposes set forth in Article SECOND. The Corporation shall have full powers of management, investment, reinvestment, and the collection of all rents, revenues, issues and profits arising therefrom.";

To delete Article THIRTEENTH of the Corporation's Certificate of Incorporation in its entirety and substitute in its place a new Article THIRTEENTH to read as follows:

"**THIRTEENTH:** To amend this Certificate of Incorporation, the Board of Directors shall adopt a resolution setting forth the amendment proposed and declaring its advisability. If a majority of the InfraGard Members Alliances (IMAs) entitled to vote, vote in favor of such amendment, the amendment shall become effective upon filing in accordance with Delaware General Corporation Law,";

To delete Article FOURTEENTH of the Corporation's Certificate of Incorporation in its entirety and substitute in its place a new Article FOURTEENTH to read as follows:

"**FOURTEENTH:** The address of its registered office in the State of Delaware is 1209 Orange Street, City of Wilmington, County of Newcastle, 19801. The name of its registered agent at such address is the Corporation Trust Co."; and

To delete Article FIFTEENTH of the Corporation's Certificate of Incorporation in its entirety and substitute in its place a new Article FIFTEENTH to read as follows:

"**FIFTEENTH:** The name and mailing address of the sole incorporator are as follows:

Willam J. Culbertson
Baker & Hostetler LLP
3200 National City Center
1900 East Ninth Street
Cleveland, Ohio 44114"; and

To delete Article SIXTEENTH in its entirety.

SECOND: That thereafter on June 29, 2004, said amendments to the Certificate of Incorporation were duly adopted by a majority vote of the local chapters of the Corporation at a regular meeting of the Corporation's members:

IN WITNESS WHEREOF, Infragard, Inc. has caused this certificate to be signed by a duly authorized officer this 20th day of July, 2004.

INFRAGARD, INC.

By: Sheri A. Donahue

Name: Sheri A. Donahue

Title: Secretary, InfraGard, Inc.

[illegible], Infragard, Inc. has caused this certificate to be signed by a duly authorized officer this 20th day of July, 2004.

Sent: Friday, August 22, 2008 12 M
To: (OGC) (FBI)
Cc: (OGC) (FBI); (CyD)(FBI)
Subject: FW: InfraGard

UNCLASSIFIED
NON-RECORD

a quick note on this topic since it has been almost a year.
Based upon what I wrote at the bottom of this email,

Please let me know your thoughts.
I'm out of the office on official travel until 9/2 after today.
Thanks for you efforts,

From: (CyD) (FBI)
Sent: Friday, September 28, 2007 3 16 PM
To: (OGC) (FBI), (D9) (FBI)
Cc: (OGC) (FBI); (DI) (FBI); (OGC) (FBI);
(OGC) (FBI); (CyD) (FBI)
Subject: RE: InfraGard

UNCLASSIFIED
NON-RECORD

thanks.
please let us know what I'm supposed to do next. I'm on official travel next week. If you need something next week, please contact A/UC Otherwise, I can get w/ you when I return.
Thanks,

-----Original Message-----
From: (OGC) (FBI)
Sent: Wednesday, September 26, 2007 2:58 PM
To: (CyD) (FBI); (D9) (FBI)
Cc: (OGC) (FBI); (CyD) (FBI); (OGC) (FBI);
(OGC) (FBI)
Subject: RE InfraGard

UNCLASSIFIED
NON-RECORD

We will put together a request for a DOJ opinion. (unfortunately for us) will soon be going to work for in OIC, so I will be reassigning this to as project attorney.

Associate General Counsel
Chief, General Law Unit (formerly Administrative Law)
935 Pennsylvania Ave. N.W., Rm 7338
Washington, D.C. 20535

[redacted] b6 b7C

-----Original Message-----
From: [redacted] (CyD) (FBI)
Sent: Wednesday, September 26, 2007 1:36 PM
To: [redacted] (OGC) (FBI)
Cc: [redacted] (OGC) (FBI) [redacted] (CyD) (FBI)
Subject: InfraGard [redacted]

b5 b6 b7C

UNCLASSIFIED
NON-RECORD

[redacted] hello. Thank you for your Unit's hard work on the complex issue [redacted]

[redacted] b5 b6 b7C

Again, thank you for your work and please let [redacted] and [redacted] know their efforts helped us move on a primary area of concern for my private sector partners.

Sincerely,

[redacted]
Unit Chief
Public/Private Alliance Unit
[redacted]

b6 b7C

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

UNCLASSIFIED

b6
b7C

SECRETARY OF STATE
DIVISION OF CORPORATIONS
FILED 05:30 PM 04/07/2003
030229511 – 3645152

CERTIFICATE OF INCORPORATION
OF
INFRAGARD, INC.

FIRST: The name of the corporation shall be Infragard, Inc. (hereafter "the Corporation").

SECOND: The Corporation is organized and shall be operated exclusively for charitable, educational, or scientific purposes within the meaning of section 501(c)(3) of the Internal Revenue Code, including, but not limited to:

1. Providing the principal trusted partnership between the private sector, government, and academia to strengthen the security of the American people;
2. Providing a forum for dialogue and relationship building between policy makers, implementers, stakeholders, and law enforcement;
3. Providing a conduit between InfraGard membership and national leaders;
4. Educating the public about the security of the United States national infrastructures;
5. Increasing the security of the United States national infrastructures through ongoing exchanges of information relevant to infrastructure protection;
6. Disseminating information related to the security of the United States national infrastructures; and
7. Conducting, sponsoring and funding meetings, programs and seminars to educate the public about the security of the United States national infrastructures.

THIRD: No part of the net earnings of the Corporation shall inure to the benefit of or be distributable to its directors, officers, members, or private individuals, but the Corporation shall be authorized and empowered to pay reasonable compensation for services rendered and to make payments and distributions in furtherance of the purposes set forth in Article SECOND hereof.

FOURTH: It is intended that the Corporation shall have and continue to have the status of a corporation which is exempt from federal income taxation under section 501(a) of the Internal Revenue Code as an organization described in section 501(c)(3) of the Internal Revenue Code. This Certificate of Incorporation shall be construed accordingly, and all powers and activities hereunder shall be limited accordingly. Notwithstanding any other provision of this Certificate of Incorporation, the Corporation shall not carry on any activities not permitted to be carried on by an organization exempt from federal income tax under section 501(c)(3) of the Internal Revenue Code.

b7E

The Corporation shall not carry on propaganda or otherwise attempt to influence legislation to such extent as would result in the loss of exemption under section 501(c)(3) of the Internal Revenue Code. No activity of the Corporation shall consist of participating in or intervening in (including the publishing or distributing of statements) any political campaign on behalf of or in opposition to any candidate for public office.

FIFTH: To further the Corporation's objects and purposes, the Corporation shall have and shall exercise all the powers conferred by the provisions of the laws of the State of Delaware upon nonprofit corporations that are consistent with the scope of Article SECOND hereof. Without limiting the generality of the foregoing, the Corporation shall have the power to sue and be sued, to own, to take title to, receive and hold, lease, sell and resell, in fee simple or otherwise, property, real, personal or mixed, wherever situated or however acquired, without limitation as to amount or value. The Corporation shall have the right, power and authority: to receive gifts, bequests and contributions outright, in trust or in any other form; to grant and exercise options to buy or sell; to encumber property by deed of trust, pledge or otherwise; to borrow money and secure payment of same by placing one or more liens on the realty and/or personal property of the Corporation; to lease, build, or erect, remodel, repair, construct and/or reconstruct any and all buildings, houses, or other structures necessary, proper or incident to the carrying out of the objects and purposes stated herein. The Corporation shall have the right, power and authority to collect dues, and to use, apply, invest and reinvest the principal and/or income therefrom or to distribute the same for the purposes set forth in Article SECOND. The Corporation shall have full powers of management, investment, reinvestment, and the collection of all rents, revenues, issues and profits arising therefrom.

SIXTH: The Corporation shall be a nonprofit corporation.

SEVENTH: The Corporation shall not have any capital stock.

EIGHTH: The conditions of membership in the Corporation shall be stated in the Bylaws.

NINTH: Except as otherwise provided for in this Certificate of Incorporation, the qualifications and rights, including voting rights, of the directors shall be as set forth in the Bylaws of the Corporation. Directors shall be elected in the manner set forth in the Bylaws. Elections of directors need not be by written ballot unless the Bylaws of the Corporation so provide.

TENTH: Upon any dissolution or final liquidation of the Corporation, the Board of Directors shall, after paying or making provision for the payment of all the lawful debts and liabilities of the Corporation, distribute all of the assets of the Corporation to such nonprofit organization or organizations that the Board of Directors determines have similar charitable, educational or scientific purposes as the Corporation and which then qualify as an organization described in 501(c)(3) of the Internal Revenue Code.

Any assets not so disposed of shall be disposed of by a court of competent jurisdiction of the county in which the principal office of the Corporation then is located, exclusively for one or more

b6
b7C
b7E

exempt purposes within the meaning of section 501(c)(3) of the Internal Revenue Code or to such organization or organizations described in section 501(c)(3) of the Internal Revenue Code as such court shall determine.

ELEVENTH: References herein to sections of the Internal Revenue Code are to provisions of the Internal Revenue Code of 1986, as amended, as those provisions are now enacted or to corresponding provisions of any future United States internal revenue law.

TWELFTH: The Corporation shall indemnify its directors and officers for the defense of civil or criminal actions or proceedings as set forth in its Bylaws, so long as such indemnification does not constitute a violation of any provision of the Internal Revenue Code applicable to an organization described in section 501(c)(3) of the Internal Revenue Code. To the fullest extent permitted by the General Corporation Law of the State of Delaware, as the same exists or may hereafter be amended, a director of the Corporation shall not be liable to the Corporation or its members for monetary damages for breach of fiduciary duty as a director, so long as such limitation on liability does not constitute a violation of any provision of the Internal Revenue Code applicable to an organization described in section 501(c)(3) of the Internal Revenue Code. Any repeal or modification of this Article shall not adversely affect any right or protection of any director of the Corporation existing at the time of such repeal or amendment.

THIRTEENTH: To amend this Certificate of Incorporation, the Board of Directors shall adopt a resolution setting forth the amendment proposed and declaring its advisability. If a majority of the Local Chapters vote in favor of such amendment and the Federal Bureau of Investigation (the "FBI") gives its written concurrence in favor of the amendment, the amendment shall become effective upon filing in accordance with Delaware General Corporation Law.

[illegible] described in section 501(c)(3) of the [illegible]

FOURTEENTH: The Board of Directors, the FBI or any Local Chapter (as defined in the Bylaws) may propose amendments to the Bylaws of the Corporation. To repeal, modify, amend the Bylaws of the Corporation or to adopt new Bylaws of the Corporation the following shall be required: the affirmative vote of (a) a majority of all directors or a majority of all Local Chapters; and (b) the written concurrence of the FBI acting through its InfraGard Program Manager. The FBI shall give strong consideration in favor of giving its concurrence to any amendment proposed by a majority of Local Chapters.

FIFTEENTH: The address of its registered office in the State of Delaware is 1209 Orange Street in the City of Wilmington, County of New Castle, 19801. The name of its registered agent at such address is The Corporation Trust Company.

[illegible]

[illegible] this Certificate of Incorporation [illegible]

[illegible]

[illegible] the FBI acting through its Infra[illegible]

SIXTEENTH: The name and mailing address of the sole incorporator are as follows:

William J. Culbertson
Baker & Hostetler LLP
3200 National City Center
1900 East Ninth Street
Cleveland, Ohio 44114

THE UNDERSIGNED, being the incorporator above named, for the purpose of forming a corporation pursuant to Chapter 1 of Title 8 of the Delaware Code, does make this Certificate, hereby declaring and certifying that the facts herein stated are true, and accordingly has hereunto set his hand this 4th day of April, 2003.

Sole Incorporator

Baker & Hostetler LLP
3200 National City Center

G:\Client\WJC\3600\Inc\Cert_Certificate of Incorporation 041104.doc

[redacted]

InfraGard Domestic Membership Application

Name (Applicant) :
Employer:
Title:
Business Address[1]:
City: State:
Zip Code:
Home Address[1]:
City: State:
Zip Code:
Chapter Selection State: Select State City:
Email Address:
Phone: Fax:
Date of Birth:
City, County, State, and Country of birth: U.S. Citizen: ☐ Yes ☐ No
Social Security Number: Driver's License Number:
Code Word.[2]

Have you ever been arrested for, charged with, or convicted of a felony or non-traffic misdemeanor? If yes, please attach an explanation of the occurrence(s) making sure to include dates, agencies involved, case numbers, disposition, and any additional information that you feel would assist us in making a membership decision (Check one):

☐ No
☐ Yes (Number of pages attached:)

Do you currently possess a Qualifying Substitute for the records check required for InfraGard Membership? (A current list of Qualifying Substitutes is available in a separate document or on the InfraGard web site):

☐ No
☐ Yes, I am an InfraGard SAA Member and already successfully completed a records check
(InfraGard Chapter: Application Date:[3])
☐ Yes, I posses a current and valid Security Clearance listed as a Qualifying Substitute
(Clearance: Issuing Agency: Expiration:)
(Security Contact:)

Which Critical Infrastructures is your organization a part of? Check all that apply:

☐ Agriculture	☐ Banking & Finance	☐ Chemical Industry & HAZMAT
☐ Defense	☐ Emergency Services	☐ Energy
☐ Food	☐ Government	☐ Information & Telecom.
☐ Law Enforcement	☐ National Monuments & Icons	☐ Postal & Shipping
☐ Public Health	☐ Transportation	☐ Water
☐ Other:		

[1] Physical street address required. No PO boxes.
[2] Authentication for Help Desk use Examples include mother's maiden name, city of birth, etc...
[3] If exact date is unknown, please provide an approximate date

If accepted as a member of InfraGard, Applicant may receive information that is sensitive and not publicly available ("Protected Information"). Protected Information may be provided by or through the InfraGard National Organization, InfraGard chapters, InfraGard members, partners of InfraGard, or other sources, and will be marked accordingly. If accepted as an InfraGard member, Applicant understands and agrees to the following terms *regarding Protected Information*

1. **Participation is Voluntary.** Applicant is not obligated as a condition of InfraGard membership to disclose any information to the InfraGard National Organization or any InfraGard chapter, partner, or member.
2. **Confidentiality and Non-Disclosure.** Protected Information is to be regarded as Business Confidential and shall not be disclosed beyond its intended scope.
3. **No guarantee of fitness.** Protected Information is provided as a service to InfraGard members and may be unevaluated and unverified. As such Protected Information is not guaranteed to be accurate, complete, or actionable.
4. **Submission in Good Faith.** Applicant agrees that it will not submit information which it knows at the time of submission to be false, and that it will submit information only to further InfraGard's stated purposes.
5. **Federal Agencies will exercise care to protect information.** To the extent allowed by law, information received from InfraGard members that is marked "InfraGard Protected Information" shall be protected from agency disclosure under 5 USC §552 (commonly referred to as the Freedom of Information Act ("FOIA")), and from publication, divulgence, or release in any other manner pursuant to the prohibitions of the Trade Secrets Act, 18 USC §1905.

Applicant understands and agrees that InfraGard is not to be commercially exploited as a forum to market products or services and that doing so may result in the revocation of Applicant's membership in InfraGard.

Applicant, if accepted as an InfraGard member, agrees to act in a manner consistent with the InfraGard National By-Laws, as the ByLaws may be amended from time to time, as well as any other duly enacted national requirements of InfraGard.

Applicant requirements:

- US Citizen by birth as defined by 8 USC §1401-§1409, OR US Citizen by Naturalization as defined by 8 USC §1421-§1459;
- Over 18 years of age on the date of completion of this Application;
- Consent to a records check that yields a satisfactory result as determined by the FBI in its sole discretion, OR posses a Qualifying Substitute;
- Consent to periodic re-confirmation of membership requirements;
- Have sponsorship from an existing InfraGard member, chapter, or partner organization;
- Agree to and complete this InfraGard Membership Application Form;
- Any further requirements (if more restrictive) mandated by the local chapter and approved by the FBI.

Applicant acknowledges that their affiliation with InfraGard may be disclosed by InfraGard to another InfraGard member, chapter, or partner. Applicant may choose to protect from *public* disclosure their affiliation with InfraGard, and request that InfraGard and InfraGard Partners also protect from public disclosure the Applicant's affiliation with InfraGard to the full extent permitted by law.

May InfraGard *publicly* disclose Applicant's association with InfraGard? (Check one):

☐ No
☐ Yes

PRIVACY ACT STATEMENT AND CONSENT

Authority:
Collection of this information is authorized under 28 CFR. § 0.85.

Principal Purpose and Routine Uses
The information collected on this form will be used for the principal purpose of conducting security risk assessments on InfraGard Members and applicants. As part of this assessment, the collected data may also be used to assist in determining approval, denial, revocation or renewal of access to the InfraGard Secure web site and the authorization to receive InfraGard sensitive information. Information provided by me will be protected and used in strict compliance with the Privacy Act and the routine uses most recently published in the Federal Register for the FBI's Central Records System (Justice/FBI-002) and the FBI's Blanket Routine Uses (Justice/FBI-BRU).

Social Security Account Number
Your Social Security Account Number (SSAN) is requested to check criminal, immigration, national security and other electronic databases. Because other people may have the same name and birth date, your SSAN will be used to facilitate accurate identification and to help eliminate the possibility of misidentification of individuals for whom a security risk assessment or database check is being conducted.

Effects of Nondisclosure or Falsification
Completion of this application and provision of your SSAN is voluntary. However, failure to provide the requested information may result in your application being rejected for membership in InfraGard or your membership revoked. Knowingly falsifying or concealing information requested on this form will result in your application being rejected or your membership revoked. In addition, Title 18 Section 1001 of the U.S. Code provides that knowingly falsifying or concealing a material fact may under certain circumstances constitute a felony resulting in fines and/or imprisonment.

Consent
By signing an InfraGard Membership Application Form, I hereby authorize the FBI to obtain and verify any information relevant to assessing my suitability to access, possess, use, receive or transfer sensitive InfraGard Information. This information may include, but is not limited to, law enforcement and intelligence information. I further authorize the FBI to disclose information obtained in connection with my security risk assessment in order to verify the accuracy or completeness of the information I have provided to the FBI. Other than to verify my information, I do not authorize the FBI to disclose for the purpose of conducting my security risk assessment information provided by me on this form absent my further written consent.

Paperwork Reduction Act Notice
The information required on this form is in accordance with the Paper Work Reduction Act of 1995. The purpose of this information is to assist the FBI in security risk assessments for entities and individuals who are InfraGard Members or applicants. The estimated average burden associated with this collection of information is 20 minutes, depending on circumstances. Comments concerning the accuracy of this burden estimate and suggestions for reducing this burden should be directed to Federal Bureau of Investigation, Records/Information Dissemination Section, 935 Pennsylvania Ave., N.W., Washington, DC 920535.

I understand that this is a legally binding document and false statements provided by me are violations of federal law and may lead to criminal prosecution or other legal action. To the best of my knowledge and belief, I affirm that a). I meet all of the requirements to be an InfraGard member; b). The information I have provided herein is true, complete and correct; and c). I have reviewed the InfraGard Code of Ethics and I agree to abide by its covenants.

_____ Date: _____
PRINTED NAME

_____ Date: _____
SIGNATURE

---------- Below this Line for FBI Use Only ----------

Special Agent in Charge or Appointed Designee: _____

Witness: _____

Instructions for PDF submission

1. Complete the application (completely fill out all fields to avoid delays).
2. Print out the application
3. Sign and Date
4. Mail to:

FEDERAL BUREAU OF INVESTIGATION
FOI,PA
DELETED PAGE INFORMATION SHEET
FOI,PA# 1643419-000

Total Deleted Page(s) 3
Page 29 ~ Duplicate,
Page 30 ~ Duplicate,
Page 31 ~ Duplicate,

XXXXXXXXXXXXXXXXXXXXXXX
X Deleted Page(s) X
X No Duplication Fee X
X For this Page X
XXXXXXXXXXXXXXXXXXXXXXX

[redacted] a quick note on this topic since it has been almost a year.
Based upon what I wrote at the bottom of this email [redacted]

[redacted]

Please let me know your thoughts.
I'm out of the office on official travel until 9/2 after today.
Thanks for you efforts, [redacted]

b5
b6
b7C

From: [redacted](CyD) (FBI)
Sent: Friday, September 28, 2007 3:16 PM
To: [redacted](OGC) (FBI); [redacted](D9) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](DI) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI); [redacted](CyD) (FBI)
Subject: RE: InfraGard [redacted]

b5
b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted] thanks.
[redacted] please let us know what I'm supposed to do next. I'm on official travel next week. If you need something next week, please contact A/UC [redacted] Otherwise, I can get w/ you when I return.
Thanks [redacted]

b6
b7C

-----Original Message-----
From: [redacted](OGC) (FBI)
Sent: Wednesday, September 26, 2007 2:58 PM
To: [redacted](CyD) (FBI); [redacted](D9) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](CyD) (FBI); [redacted](OGC) (FBI); [redacted](OGC) (FBI)
Subject: RE: InfraGard [redacted]

b5
b6
b7C

UNCLASSIFIED
NON-RECORD

[redacted]

b6
b7C

We will put together a request for a DOJ opinion. [redacted] (unfortunately for us) will soon be going to work for [redacted] in OIC, so I will be reassigning this to [redacted] as project attorney.

[redacted]

b5

[redacted]

Associate General Counsel
Chief, General Law Unit (formerly Administrative Law)
935 Pennsylvania Ave. N.W., Rm 7338
Washington, D.C. 20535

b6
b7C

[redacted]

-----Original Message-----
From: [redacted](CyD) (FBI)
Sent: Wednesday, September 26, 2007 1:36 PM
To: [redacted](OGC) (FBI)
Cc: [redacted](OGC) (FBI); [redacted](CyD) (FBI)
Subject: InfraGard [redacted]

b5
b6
b7C

b5
b6
b7C

[redacted] hello. Thank you for your Unit's hard work on the complex issue [redacted]

[redacted]

Again, thank you for your work and please let [redacted] and [redacted] know their efforts helped us move on a primary area of concern for my private sector partners.

Sincerely [redacted]

[redacted]
Unit Chief
Public/Private Alliance Unit
[redacted]

b6
b7C

UNCLASSIFIED

UNCLASSIFIED

Information Technology Bulletin
Commonwealth of Pennsylvania
Governor's Office of Administration/Office for Information Technology

ITB Number:	ITB-PLT013
ITB Title:	Use of Freeware Policy
Issued by:	Deputy Secretary for Information Technology
Date Issued: November 20, 2006	**Date Revised:**
Domain:	Platform
Discipline:	Platform
Technology Area:	Software

Abstract:

The purpose of this Information Technology Bulletin (ITB) is to implement policy regarding the use of freeware by Commonwealth agencies. *Freeware is unsupported software that is available free of charge and can be used for unlimited time in a manner consistent with its end-user agreement.* It is important to understand that since freeware software is not officially supported by an individual entity or community, all associated risks involved with using freeware fall solely on the end user. In addition, when considering the use of a freeware product it is critical that the end-user agreement is understood and complied with as it often imposes certain restrictions such as "non-commercial use," meaning that it is not suitable for use by business and/or government agencies. Other considerations include product validation and inherent security risks. Freeware does not offer guarantees on functionality and cannot be validated to ensure that the end user knows exactly what they are obtaining. It is typically distributed without its source code, which prevents examination and modification by its users.

It is important to note that freeware is not to be confused with "open source" software, which is normally free GNU/GPL-supported software whose source code is published and made available to the public, nor is it to be confused with shareware, which is licensed, trial-version software that can be used free for a limited period of time. Both of these classes of free software differ from "freeware" in that they offer more reliability in areas of support and validation through the licenses by in which they are governed.

Agency Use of Freeware

Freeware offers potential users the benefit of using various programs without having to pay fees. Agency users may decide a particular freeware utility offers certain advantages not found in any of the current enterprise software products, but will still be tied to the stipulations of the freeware end-user agreement. It is important to understand that there may be legal liabilities for any usage that violates the terms of the agreement.

Inherent Security Vulnerabilities

Since freeware software lacks guaranteed support from a software vendor or the type of support GNU/GPL-licensed software receives from the open source community, it is unknown what vulnerabilities may exist in the underlying source code of the program. Embedded spyware/malware, Trojan horse programs, and macro execution are some examples of typical attack vectors that can be embedded within freeware and can often pass through anti-virus scans undetected. Because of the unknown nature of the underlying code in freeware software, allowing untested

use of it in a production environment may pose an unacceptable security risk to Commonwealth assets and infrastructure.

Support Issues
Although freeware is free and does not carry a price tag *per se*, there are other costs and risks that need to be factored in when considering total cost-of-ownership. Typical compatibility issues experienced over time with other co-existing applications can be a particular problem for freeware applications. Since freeware applications are unsupported, there may be no way of resolving an issue other than trying to uninstall the program, which may or may not be easily accomplished. In addition, as newer versions of applications are rolled out through typical software lifecycles, upgrades to co-existing applications may need to take place to ensure compatibility. With freeware, users run the risk of not being able to obtain later versions when the product eventually becomes obsolete. The bottom line is that unsupported software can result in a costly interruption to service if it is too heavily depended upon or used in a way that creates interdependencies with other business applications.

General:
This ITB applies to all departments, boards, commissions and councils under the governor's jurisdiction. Agencies not under the governor's jurisdiction are strongly encouraged to follow this policy.

Policy:
This policy in this ITB will address freeware in the context as defined above.

The Office of Administration/Office for Information Technology (OA/OIT) prohibits the use of freeware software not already adopted as a current product standard in any of the existing OA/OIT Information Technology Bulletins.

Agencies wishing to deploy freeware that conflicts with this policy are to submit a waiver request and obtain approval from the Technical Architecture Review Board before installation of any product.

Agencies are solely responsible to ensure that the use of freeware will not invalidate the terms as specified in the end-user agreement and that the product does not conflict with existing support agreements. Agencies granted approval to use a freeware application are to have their appropriate legal office review the terms of the product agreement to ensure they are acceptable to the Commonwealth.

Agencies are responsible for support and inventory control of freeware products. Freeware products to be used in production are to be tested and validated in a development environment to ensure security and quality control.

Trial version software is not considered freeware as defined by this policy and may be used for limited testing in production environments without going through the waiver process.

Refresh Schedule:
All standards identified in this ITB are subject to periodic review and possible revision, or upon request by the Enterprise Architecture Standards Committee (EASC).

Exemption from This Policy:

In the event an agency chooses to seek an exemption for reasons such as the need to comply with requirements for a federally mandated system, the waiver section of the IT Procurement/Waiver Review Form is to be completed and submitted to the appropriate agency Community of Practice (CoP) Planner.

Questions:

Questions regarding this policy are to be directed to ra-oaitb@state.pa.us.

References:

ITB PLT001: Desktop and Laptop Technology Standards.

History

- Created in 1996
- 83 of the top 100 firms in the Fortune 500 have an InfraGard representative
- How to become a member

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI sponsored program, and will work with DHS in support of its CIP mission, facilitate InfraGard's continuing role in CIP activities, and further develop InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

Goals & Objectives

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The relationship supports information sharing at national and local levels and its objectives are as follows:

- Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs.

- Increase interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.

- Provide members value-added threat advisories, alerts, and warnings.
- Promote effective liaison with local, state and federal agencies, to include the Department of Homeland Security.
- Provide members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

Local Chapter Activities

Each FBI Field Office has a Special Agent Coordinator who gathers interested companies of various sizes from all industries to form a chapter. Any company can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. The following illustrates additional activities that local chapters may offer:

- Training and education initiatives
- A local newsletter
- A Contingency Plan for using alternative systems in the event of a successful large scale attack on the information infrastructure

InfraGard Board of Directors

InfraGard members are represented nationally by an elected board of seven representatives called the InfraGard Board of Directors. Elections are held annually at the InfraGard National Congress for voluntary two-year terms. The Board is responsible for representing the membership in the partnership with the FBI. They conduct weekly conference calls to address a variety of issues that face the organization. Board members travel to various chapter activities and attend conferences promoting InfraGard and other issues pertinent to the program.

The Board established several committees to address issues such as membership, incorporation, and partnerships with other private sector associations/organizations. Special Interest Groups (SIGs) have also been established to meet the challenges America faces in protecting against criminal, terrorist, and intelligence threats. One such SIG involves InfraGard, the National Institute of Standards and Technology (NIST), the Small Business Administration, and the FBI.

InfraGard Secure Web Site

The InfraGard secure website provides members with information about recent intrusions, research related to critical infrastructure protection, and the capability to communicate securely with other members.

InfraGard New Coordinator Handbook

SAC/ADIC Packet

History

InfraGard is a Federal Bureau of Investigation (FBI) program that began in the Cleveland Field Office in 1996. It was a local effort to gain support from the information technology industry and academia for the FBI's investigative efforts in the cyber arena. The program expanded to other FBI Field Offices, and in 1998 the FBI assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC) and to the Cyber Division in 2003. InfraGard and the FBI have developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters.

Program Description

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with Supervisory Special Agent Program Managers in the Cyber Division at FBI Headquarters in Washington, D.C.

Each field office participates in the InfraGard Program by promoting, maintaining, and supporting one or more InfraGard Chapters within the field office territory. A local InfraGard chapter is a partnership, which facilitates the exchange of information between the FBI, an InfraGard Members Alliance (IMA), and chapter members, the owners and operators of the local and national critical infrastructure. In the spirit of partnership each chapter addresses the concerns of all chapter partners who work together for mutual benefit within the information-sharing context. As a partner, the field office assists with and promotes projects proposed by other local chapter partners. Local IMAs elect members for a national board, called the InfraGard National Membership Association (INMA) The INMA consist of seven representatives whose titles are president, vice-president, secretary, treasurer and three directors. They work directly with a designated InfraGard Program Manager at FBI Headquarters in Washington, DC. The INMA, nationally and through its local InfraGard Members Alliances, represents the programs interests of the thousands of private sector InfraGard members located throughout the United States.

Mission

While under the direction of NIPC, the focus of InfraGard was cyber infrastructure protection. After September 11, 2001 NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

The mission of the InfraGard program is to support an information sharing partnership between private and public sector for the purpose of protecting the nation's critical infrastructures against attack or failure caused by either foreign or domestic threats, and to

support all FBI investigative programs, especially Counterterrorism, Counterintelligence and Cyber Crime or the top three current priorities.

InfraGard's primary mission is to prevent attacks against our infrastructure by fostering the exchange of information between law enforcement and the owners and operators of our nation's critical infrastructure in order to identify, investigate and counter those groups and individuals who threaten the American people and our economy. InfraGard also promotes and facilitates the exchange of information amongst and between the private sector and the Department of Homeland Security, international, federal, state and local entities, in order to reduce and eliminate infrastructure vulnerabilities, and to mitigate consequences.

Critical Infrastructure Sectors and Key Resource Categories

In March 2003, NIPC was transferred to the Department of Homeland Security (DHS), which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI sponsored program, and works with DHS in support of its CIP mission, facilitates InfraGard's continuing role in CIP activities, and further develops InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

DHS is the agency which identifies the official list of sectors. As of 6/1/2004, the list of critical infrastructure sectors is as follows:

1) Agriculture, Food (Meat, Poultry, Egg Products)
2) Public Health, Healthcare, Food (Other than Meat, Poultry, and Egg products)
3) Drinking Water and Water Treatment Systems
4) Energy (Except Commercial Nuclear Power Facilities)
5) Banking and Finance
6) National Monuments and Icons
7) Defense Industrial Base
8) Information Technology
9) Telecommunications
10) Chemical
11) Transportation Systems
12) Emergency Services
13) Postal and Shipping

In addition to the above critical infrastructure sectors, the following Key Resources categories are of equal focus for the purposes of critical infrastructure protection:

1) Dams
2) Government Facilities
3) Commercial Facilities
4) Nuclear Reactors, Materials, and Waste

Goals & Objectives

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. InfraGard members gain access to information that enables them to protect their assets and in turn give information to the government that facilitates its responsibilities to prevent and address terrorism and other crimes.

The relationship supports information sharing at national and local levels and its objectives are as follows:

- Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime and other major crime programs.
- Increase interaction and information sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.
- Provide members value-added threat advisories, alerts, and warnings.
- Promote effective liaison with local, state and federal agencies, to include the Department of Homeland Security.
- Provide members a forum for education and training on counterterrorism, counterintelligence cyber crime and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

FBI Field Office Management and InfraGard

While the day-to-day workings of the InfraGard Program are the responsibility of the agent FBI coordinator, FBI managers at all levels are encouraged to become involved in InfraGard activities. The Assistant Director or Special Agent in Charge of a field office should meet with InfraGard members at least annually, and should view contact with InfraGard as an opportunity to engage a supportive citizenry in understanding and assisting with the FBI's priorities. ASACs and SSAs responsible for the InfraGard Program as well as ASACs and SSAs who want to communicate the particular responsibilities of their investigative squads should utilize the unique, positive relationships developed with the InfraGard members.

Other benefits for the front office are:

- Private sector contacts which apply to front office liaison contacts.
- Point of contact which can assist in a crisis situation.
- Information flow available from the community to the field office.
- Point of contact from all the infrastructure sectors and key resources in the division.
- Enhances the image of the FBI and field office within the community and demonstrates the willingness of the field office in opening the lines of communication.

Local Chapter Activities

Each FBI Field Office has a Special Agent Coordinator who gathers interested companies of various sizes from all industries to form a chapter. Any company and United States citizen can join InfraGard. Local executive boards govern and share information within the membership. Chapters hold regular meetings to discuss issues, threats and other matters that impact their companies. Speakers from public and private agencies and the law enforcement communities are invited. The following illustrates additional activities that local chapters may offer:

- Training and education initiatives
- A local newsletter
- A Contingency Plan for using alternative systems in the event of a successful large scale attack on the information infrastructure

InfraGard Board of Directors

InfraGard members are represented nationally by an elected board of seven representatives called the InfraGard Board of Directors. Elections are held annually at the InfraGard National Congress for voluntary two-year terms. The Board is responsible for representing the membership in the partnership with the FBI. They conduct weekly conference calls to address a variety of issues that face the organization. Board members travel to various chapter activities and attend conferences promoting InfraGard and other issues pertinent to the program.

The Board established several committees to address issues such as membership, incorporation, and partnerships with other private sector associations/organizations. Special Interest Groups (SIGs) have also been established to meet the challenges America faces in protecting against criminal, terrorist, and intelligence threats. One such SIG involves InfraGard, the National Institute of Standards and Technology (NIST), the Small Business Administration, and the FBI.

LSU Responsibilities

With the creation of DHS in March 2003, LSU has become the main point of contact for membership and coordinators. LSU houses the servers and serves as the program office.

The InfraGard staff at LSU oversees most program issues including the following items:
Entry, processing and completion of membership applications,
Create, modify e-mail accounts and passwords,
Receive, format and upload web content for all program related websites (including 24x7 content pager duties),
Responds to all inquiries made directly to the national program,
Creation and distribution of printed material, including welcome packet, cds, brochures,
Creation and moderation of listservs,
Technical support for e-mail, web access and associated issues.

InfraGard Web Sites

Currently the InfraGard program has two separate websites - all maintained by LSU.

VPN Secure Site – http://www.infragard.org
Commonly referred to as the new site. Users can only get to this site by using VPN. Secure members are issued a user id and password for site access.

This website is updated daily including news articles, governmental newsletters, security reports. More than 800 news articles are posted every month.

Major topics found on the secure site are as follows: Alerts & Advisories * Agriculture * Banking and Finance * Chemical Industry * Computer Security * Emergency Services * Defense * Homeland Security * Energy *Food * Postal and Shipping * Public Health * Transportation * Telecommunications * Water Supply

Public website - www.infragard.net
General information about InfraGard available to anyone.

Chapter websites
Many local chapters run their own websites posting information vital to chapter activities. Maintained by local chapter individuals.

Frequently Asked Questions

Q: What is InfraGard?

A: A government and private sector alliance. InfraGard was developed by FBI Cleveland in 1996 to promote protection of critical information systems. InfraGard provides formal and informal channels for the exchange of information about infrastructure threats and vulnerabilities.

Q: Why do we need InfraGard?

A: InfraGard is needed for several reasons:

- Most infrastructure components are privately owned and operated;
- The government and the private sector have a wealth of information on threats to our systems, and this wealth needs to be shared and analyzed;
- Systems are often interconnected;
- Reliance on automation is increasing;
- Tools to do harm are widely available and do not require a high degree of technical skill;
- Globalization of infrastructures increases exposure to potential harm;
- Sophisticated communication systems in the hacker community; and
- Victims often do not report cyber intrusions (Institutional concerns about the outcome and confusion about when/where to report the incident)

Q: Which threats does InfraGard address?

A: Unstructured Threats (Insiders, Recreational Hackers, and Institutional Hackers); Structured Threats (Organized Crime, Industrial Espionage and Terrorists); and National Security Threats (Intelligence Agencies and Information Warriors).

Q: How does the government benefit from InfraGard?

A: The benefits are:

1. More computer intrusions are reported;
2. Satisfies PDD-63 requirement for the FBI to play an active role in protecting our critical infrastructures;
3. New channels to disseminate threat warnings to the private sector and other government agencies;
4. New contacts in the business community;
5. Prompt threat warnings from the FBI and other InfraGard members;
6. Better understanding of the FBI and other law enforcement resources available to combat cyber and physical threats;
7. Education and training on cyber and physical security topics; and
8. The opportunity to interact and share information with representatives from the law enforcement community, academia, private industry, and other government agencies.

- An example of the working relationship between the FBI and InfraGard chapters is best represented in the power outages in August of 2003. The New York Metro Chapter was contacted by FBI officials to determine whether the power outage was due in any part to terrorist activities. Based in part on information received from the InfraGard chapter, it was determined not to be a terrorist attack.

Benefits for Members

- FBI Certified and Accredited System
- Approved for sensitive but unclassified information
- Accessible from any internet connection
- VPN Technology
- No cost to user
- VPN software provided to user
- Secure e-mail communication
- Host based virus scanning of e-mail
- Secure online information sharing environment
    - Library articles
    - Periodicals
    - DHS Alerts and Advisories

CYBER DIVISION

Public/Private Alliance Unit

The mission of the Public/Private Alliance Unit is to develop partnerships between the FBI and private sector, academic, and other public entities, to support the Cyber Division National Strategy and the FBI's Counterterrorism, Counterintelligence and other priority investigative programs.

The Cyber Division recognizes the distinct advantages of enhancing cooperation with the private sector, including the high-technology industry and academia, where prudent, in combating emerging cyber-based terrorist, foreign intelligence, or criminal threats. Within both formal and informal settings, these include expanding the FBI's knowledge of national security cyber threats and online criminal activities by facilitating effective information sharing protocols with the private sector, improving FBI technical capabilities by benefiting from the expertise and knowledge of the private industry in a rapidly changing technical environment, and by leveraging FBI training resources where possible.

As such, the Public/Private Alliance Unit (PPAU) keeps apprized of and fosters Cyber Division liaisons, companies, academic institutions, partnerships, and collaborative projects, which allows all FBI personnel to identify Division activities and endeavors.

The National InfraGard Program is at the forefront of the Public/Private Alliance Unit's efforts.

InfraGard is an FBI program that began in the FBI's Cleveland Office in 1996. In 1998, InfraGard was assigned a Program Manager from FBI Headquarters and has since developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard's information sharing and analysis effort serves the interests and combines the knowledge base of a wide range of its 84 Chapters and 11,500 plus vetted members.

The goal of InfraGard is to promote ongoing dialogue and timely communication between members and the FBI. This information sharing is primarily accomplished by InfraGard Chapters, which are geographically linked with FBI Field Office territories and their dedicated FBI Special Agent Coordinators. It is also accomplished by the PPAU with the distribution of the intelligence communities Bulletins, Assessments, and Intelligence Information Reports. Any critical infrastructure owners and operators can join InfraGard and participate in local chapter training and education initiatives, receive newsletters, and participate in meetings. The InfraGard Secure Website, supported by Louisiana State University, is a Virtual Private Network, which includes email to enable members and the FBI to exchange sensitive, unclassified information.

Please visit the InfraGard public website to view initiatives and activities: www.InfraGard.net.

FEDERAL BUREAU OF INVESTIGATION

Precedence:
DEADLINE 04/28/2006 Date: 03/07/2006

To: All Field Offices Attn: ADICs/SACs
ASACs
Cyber SSAs
InfraGard Coordinarors
FBIHQ, Manuals Desk

From: Cyber
Information Sharing and Analysis Section
Public/Private Alliance Unit, Room 5842
Contact: Unit Chief [redacted]

Approved By: [redacted] b6 b7C b7E

Drafted By: [redacted]

Case ID #: [redacted] b3 b7E
66F-HQ-C1384970

Title: SEMIANNUAL REPORT;
INFRAGARD PROGRAM;
REPORTING PERIOD
10/01/2005 - 3/31/2006

Synopsis: This EC serves as the cover communication for the attached sample Semiannual InfraGard Program Report.

Enclosure(s): One sample Semiannual Report (SAR).

Details: As all field offices are aware, InfraGard is an information sharing network between the public and private sector in the form of InfraGard chapters in all FBI field offices supported by FBI Special Agent InfraGard Coordinators.

Management of the InfraGard Program at FBIHQ is in the Public/Private Alliance Unit (PPAU), Information Sharing and Analysis Section, Cyber Division. The mission of the PPAU is to develop partnerships between the FBI and private sector, academia, and other public entities, to support the Cyber Division National Strategy and the FBI's Counterterrorism, Counterintelligence, and Criminal Investigative programs.

PPAU has reviewed the SARs for the period of 4/1/2005 to 9/30/2005. The reports have provided FBIHQ management with a better understanding of the status of the InfraGard chapters

across the country. The reports have also been utilized to provide input to the inspection staff prior to field office inspections and for reference during SAC briefings. The SAR should be viewed by the field offices as a way to "self inspect" and document the overall success and shortcomings of their InfraGard chapters. As a result, PPAU encourages all field offices to utilize the SARs to conduct a thorough assessment of their InfraGard Program.

It is imperative that all field offices continue to enhance their InfraGard chapters in order to face the challenges that lie ahead. InfraGard is a critical intelligence component in the FBI, due to the expansion of InfraGard's mission to support all FBI investigative programs, including Counterterrorism, Counterintelligence, Criminal, and Cyber Crime.

Field Office executive management is encouraged to regard InfraGard as a powerful tool. Presently, InfraGard has approximately 14,000 members in 84 chapters ranging from representatives of Fortune 500 companies to the owners of small ISPs. The InfraGard membership regularly provides intelligence and referrals which assist law enforcement in its efforts to identify and counter the most significant criminal and national security threats to our country's networks.

PPAU SSAs will provide feedback via email to each field office after reviewing the Semiannual Report.

LEAD(s):

Set Lead 1: (Action)

ALL RECEIVING OFFICES

Complete a SAR, for the period of 10/1/2005 - 3/31/2006, for each InfraGard chapter in the division's territory and forward the results to PPAU, Room 5842, FBIHQ by 04/28/2006.

♦♦

b6
b7C

InfraGard Membership Database

The Application Process and How It Affects FBI Coordinators

[redacted]

Submission of New Applications

- Any application may be submitted to Louisiana State University (LSU) via US mail, FedEx, UPS, or fax. Applications submitted via fax should be followed by an e-mail or phone call to ensure proper receipt.

Send to:

InfraGard Program

402 Johnston Hall

Baton Rouge, LA 70803

Fax: (225)578-9235

Field Requirements for Application Submission

- All applications must be accompanied with the Field File Number.
- All applications must be typed to ensure legibility when being entered into the database.
- All fields on the application must be completed, including codeword, SSN, DOB, and POB.
- All applications must contain a physical mailing address. (PO Boxes will not be accepted.)

Application Process

- A member applies at www.infragard.net and mails the application into the Field Office that corresponds with his/her chapter.
- The Coordinator makes a copy of the application and sends it to LSU (the Coordinator keeps the original).
- While LSU is entering the application into the database, the Coordinator is running the appropriate background checks (see the Standardized Records Check Form).
- Application is entered into the database and goes to the Coordinator Queue (go to www.infragard.org, click on "Coordinator's Area", and "Database Login" to access your queue…the tool bar across the top reads "My Queue").
- Based on the records check, the Coordinator has the option to: Approve, Approve with Derogatory Information, or Disapprove with Derogatory Information the member out of the Coordinator Queue.

Application Process (continued)

- If the member is Approved, he/she enters the Membership Queue and is sent a Welcome Packet by LSU.
- If a member is either Approved with Derogatory Information or Disapproved with Derogatory Information, he/she will enter the Headquarters Queue.
- The Coordinator must submit an EC to FBIHQ containing information on the member if they are Approved with Derogatory Information or Disapproved. FBIHQ will decide whether a member is going to be approved or disapproved based on the EC and the Coordinator's recommendation in the field. Disapproved members receive a letter from FBIHQ.

What happens if a Welcome Packet is returned to LSU?

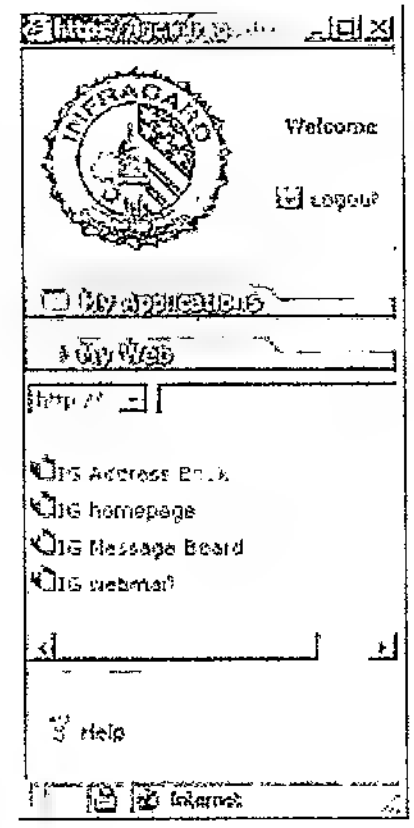
- In the event that LSU is contacted by FedEx concerning an undeliverable address, they will attempt to obtain the correct information directly from the member. However, if LSU is unsuccessful in their attempts, the package is sent to the Coordinator at the corresponding field office for further distribution.

Approval Process

1. Open a browser window.
2. Navigate to the URL: http://igc.infragard.org.
3. Click "Yes" on the Security Alert dialogue box. If additional prompts appear, click "Yes".
4. Enter your current InfraGard user name and password.
5. Click "OK" to close the browser window.

Approval Process (continued)

This launchpad will appear on the screen:



Approval Process (continued)

- Click on "IG Address Book".
- Click on "Coordinator's Area" and enter your InfraGard user name and password.
- Select "Database Login".
- It will prompt to re-enter your InfraGard user name and password. After your information is entered, click on "Login". **Do not hit Enter or you will continually be reprompted to login.**

Accessing the Coordinator Queue

- Once you enter the database, the tool bar along the top will give you an option for "My Queue".
- Open the Queue, and a list of members awaiting approval will appear.
- To move a member out of your Queue, select the "Action" link.
- You will now be required to Approve, Approve with Derogatory Information, or Disapprove with Derogatory Information (see the previous slides).

General Contact Information at LSU

Membership Issues

infragardteam@infragard.org

Content Issues

infragardcontent@infragard.org

24/7 Technical Support

877.861.6298

In addition to the membership process, LSU provides other resources to the InfraGard Coordinator in the field. Two of the most useful resources are the local chapter listserv and the local chapter website.

What is a Listserv?

A listserv is essentially an electronic mailing list of e-mail addresses of members interested in a certain topic or specific area of interest. The purpose is to enable listserv subscribers to receive daily news, bulletins, alerts or general communication from the InfraGard Program Office or their local InfraGard chapter Coordinators.

LSU has set up a listserv for each Coordinator's chapter, as well as for the local executive board of each chapter. If you would like to utilize your listserv, please contact LSU. You will be listed as the Administrator, and you can choose any number of chapter members to serve as Moderators of the listserv, if necessary. You may also request a report containing the e-mail addresses of all of your chapter members, in order to populate your listserv.

How do I setup my chapter website?

LSU has the ability to setup and maintain all local chapter websites. If your chapter does not have its own webmaster, contact LSU to run your website at no charge. There is a main template of all LSU-run websites, but each chapter adds its own individual graphics, text, and contact information to set it apart from all others. It is up to the Coordinator and the local chapter executive board to populate your site. For more information on local chapter websites, contact infragardcontent@infragard.org.

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 05/12/2005

To: All Field Offices **Attn:** InfraGard Coordinators
Community Outreach

Specialist/Coordinators

FBIHQ, Manuals Desk

From: Director's Office
Cyber
Office of Public Affairs/ Community Relations
Unit/ Room 7366; Outreach, Capability and
Section/PPAU/Room 5842 Development
Contact: SSA [redacted]
PAS

b6
b7C
b7E

Approved By: Chandler Cassandra M

[redacted]

Drafted By: [redacted]

Case ID #: [redacted]
66F-HQ-C1384970
[redacted]

b3
b7E

Title: CITIZENS' ACADEMY
INFRAGARD PROGRAM
PARTNERSHIP

Synopsis: The purpose of this EC is to notify all field office Community Outreach Coordinators/Specialists and InfraGard Coordinators of the newly established partnership between the Citizens' Academy (CA), Community Relations Unit and the InfraGard Program (IP), Public Private Alliance Unit (PPAU).

Enclosure(s): One copy of the standardized record checks form.

Details: For the information of the receiving offices, on 4/21/2005 AD Cassandra Chandler, Office of Public Affairs (OPA) met with OPA Section Chief Michael Kortan, Acting Unit Chief [redacted] Public Affairs Specialists [redacted] from the CRU, and SSA [redacted], InfraGard Program Manager, PPAU, concerning a partnership between the Citizens' Academy and the InfraGard Program. It was determined that such a partnership will

b6
b7C

strengthen the FBI's ability to build trust and improve information sharing between the Bureau and private sector leaders in support of the FBI's counterterrorism, counterintelligence, and cyber missions.

Citizens' Academy

The Citizens' Academy affords business and community leaders an inside look at Federal law enforcement in general and the FBI in particular. The eight-week (10-session) Academy gives citizens an overview of FBI and Department of Justice policies and procedures. The Academy classes are taught by FBI executives and senior FBI Special Agents, and the curriculum and teaching methods are similar to the traditional methods used at the FBI Academy. Students participate in firearms demonstrations and practical problems involving the collection and preservation of physical evidence. Students have the opportunity to meet the SAC and are encouraged to ask questions and express their concerns.

It is the goal of the FBI's Citizens' Academy to promote a greater understanding of the role of Federal law enforcement in the community through frank discussion and education. The relationships fostered through this program improve the Bureau's ability to solve/detect crimes, and help citizens' make their communities a better and safer place.

National Citizen's Academy Alumni Association

The National Citizens' Academy Alumni Association (NCAAA) is a network of FBI Citizens' Academy Alumni organizations and community-based and supported organizations, distinct and separate from the FBI. The NCAAA promotes the importance of the FBI Citizens' Academy and FBI Citizens' Academy Alumni organizations as community ambassadors who educate local communities about federal law enforcement issues and challenges. The NCAAA also supports other worthwhile community-based initiatives.

InfraGard Program

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. InfraGard is an association of business, academic

institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Each InfraGard Chapter has an FBI Special Agent Coordinator assigned to it, and the FBI Coordinator works closely with SSA Program Managers in the Cyber Division at FBI Headquarters.

Mission

A proposal was made by PPAU to establish a partnership between the Citizens' Academy and InfraGard Program, two FBI outreach initiatives responsible for engaging the private sector and community leaders across the country.

After reviewing the proposal and the responsibilities associated with the Citizens' Academy and the InfraGard Program, AD Chandler, OPA and AD Reigel, Cyber Division, agreed to establish a partnership between the two programs.

The partnership will support the mission of both the Citizens' Academy and the InfraGard Program. The objectives are as follows:

- Increase the level of information and reporting between InfraGard members (IM), Citizen Academy Alumni (CAA), community leaders, and the FBI on matters related to Counterterrorisn, counterintelligence, Cyber crime and other FBI priority programs.

- Increase communication and information sharing among IM, CAA, community leaders and the FBI regarding threats that impact the FBI's law enforcement mission.

- Promote effective liaison with local, state and federal agencies, to include business and community leaders.

- Enhance the image of the FBI and its field office within the community and demonstrate the willingness of the field office in opening the lines of communication.

In order to establish a successful partnership and to gain the maximum benefit from it, field offices are advised to follow the following guidelines and recommendations:

1. Effective immediately, a minimum of two slots should be allocated for InfraGard members in each Citizens' Academy class.

2. InfraGard Coordinators are to be notified by the Community Outreach Coordinator/Specialist when a decision has been made to conduct a Citizens' Academy class. Upon notification, the InfraGard coordinator should advise the local InfraGard Chapter of the upcoming class and establish a deadline to accept applications for the class. Once the applications are received, the InfraGard Coordinator should rank the applicants and provide a list of names (maximum of ten) in the order that they would recommend for approval by the SAC. The SAC or his/her designee will make the final determination on who is selected to participate from the InfraGard applicants. It should be noted that this does not preclude InfraGard members from applying to participate in a Citizens' Academy via the normal process.

3. Each Citizens' Academy curriculum should include a 30-45 minute InfraGard presentation to be given by the InfraGard coordinator.

4. Citizens' Academy graduates will be offered the opportunity to become a member of InfraGard without going through the standard InfraGard application process, since they have already been vetted through the Citizens' Academy application process.

5. Community Outreach Coordinators/Specialists and InfraGard Coordinators should seek out opportunities to work together and to exchange information on best practices for outreach to the local community, sources of funding for outreach activities, and other matters of joint interest.

6. Community Outreach Coordinator/Specialists and InfraGard Coordinators should cross-train where such training is applicable to both positions and where cross-training presents efficiencies or other benefits.

Administrative

A standardized record check formed has been approved for immediate use by both outreach programs when conducting the background checks on applicants. This new form was created to ensure that both programs conduct identical record checks. This will alleviate the need for additional checks to be done by either program when members are selected to participate in either of the two programs.

LEAD(s):

Set Lead 1: (Action)
ALL RECEIVING OFFICES

All receiving offices are requested to implement the partnership program, which includes the standardized record check form, allotted three slots for InfraGard members, and InfraGard presentation to be given by the InfraGard Coordinator.

Set Lead 2: (Action)

DIRECTOR'S OFFICE

AT OPA

To provided an opinion whether there are any prohibitions or considerations that would preclude the Citizens' Academy Program from partnering with the InfraGard Program.

Set Lead 3: (Action)

CYBER

AT PPAU

To provided an opinion whether there are any prohibitions or considerations that would preclude the InfraGard Program from partnering with the Citizens' Academy Program.

b6
b7C

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 08/15/2005

To: Records Management Attn: Manuals Desk
Room 6094

From: Cyber
Outreach, Capability and Development Section
Public Private Alliance Unit (PPAU), Room 5842
Contact: UC [redacted]

Approved By: [redacted]

b6
b7C
b7E

Drafted By: [redacted]

Case ID #: 66F-HQ-A1192083 [redacted]

b3
b7E

Title: PROPOSED CHANGE IN
MANUAL OF INVESTIGATIVE OPERATIONS AND GUIDELINES (MIOG);

Synopsis: To recommend procedural and policy changes in the MIOG classification [redacted] INFRAGARD.

Details:

REASON FOR CHANGE:

The realignment of the National Infrastructure Protection Center (NIPC) with the Department of Homeland Security (DHS), and the development of the InfraGard Program solely under the FBI's Cyber Division necessitates the publication of an InfraGard manual section to provide guidance to the field regarding the InfraGard Program. The [redacted] classification was approved and has replaced the 294 classification. The manual instructions for the 294 classification are to be removed from the MIOG and replaced by the classification [redacted] These changes have been coordinated with the Manuals Desk.

b3
b7E

CHANGE: Effective September 1, 2005

CHANGED TEXT

The following represents an outline of the [redacted] instructions:

SECTION [redacted] INFRAGARD
- 1 SCOPE
- 2 KEY TERMS AND ACRONYMS
- 4 SUMMARY OF LEGAL AUTHORITIES
- 5 POLICIES
  - 5.1 Membership Criteria
  - 5.2 Member Conduct: Suspension or Removal of Members
  - 5.3 FBI Field Office Management and InfraGard
  - 5.4 InfraGard Chapter Activities
  - 5.5 InfraGard Program Activities
  - 5.6 InfraGard Coordinator
  - 5.7 Classification
  - 5.8 Previous Classification
- 6 ROLES AND FUNCTIONAL RESPONSIBILITIES
- 7 RECORDKEEPING REQUIREMENTS
- 8 PROCEDURES AND PROCESSES
  - 8.1 Maintaining a [redacted] Control File
  - 8.2 Membership Processes and Procedures
  - 8.3 Public Relations and FBI Education Processes
  - 8.4 Recognition of Members
  - 8.5 Intelligence/Investigative Processes
  - 8.6 FBI Intelligence Inquiries Process
  - 8.7 Communications and Reports Processes
    - 8.7.1 Membership Application Process
    - 8.7.2 InfraGard National Database
    - 8.7.3 E-mail Communications
    - 8.7.4 Semiannual Summary Reports

b3
b7E

b3
b7E

MIOG, PART 1, SECTION [redacted] should read as follows: b3 b7E

SECTION [redacted] INFRAGARD
(FORMERLY CLASSIFICATION 294--SEE
MIOG, PART 1, SECTION 294.)

[redacted]-1 SCOPE

(1) PURPOSE: To set forth the development and implementation of the InfraGard program to ensure proper policies and procedures are followed.

(2) BACKGROUND: InfraGard is an FBI program that began in 1996 in the Cleveland Office as an effort to gain support from the information technology industry and academia for FBI investigations of threat to the cyber infrastructure. In 1998, the FBI created the 294 classification and expanded the program to other field offices and assigned national program responsibility for InfraGard to the former National Infrastructure Protection Center (NIPC). After the events of 9/11/2001, the InfraGard program was expanded to include threats to the physical infrastructure. In March 2003, NIPC was transferred to the Department of Homeland Security. In March 2003, the 294 classification was replaced by the [redacted] classification for use in InfraGard cases. b3 b7E

InfraGard is now dedicated to promoting ongoing dialogue and timely communication between the private sector and local, state, federal, and international entities regarding critical infrastructure protection. The FBI and InfraGard members are engaged in this cooperative undertaking in recognition that a public/private partnership is of vital importance to our nation's security.

(a) Primary Focus: InfraGard's primary focus is to prevent attacks against our infrastructure by fostering the exchange of information between law enforcement and the owners and operators of our nation's critical infrastructure in order to identify, investigate, and counter those groups and individuals who threaten the American people and our economy. InfraGard also supports the Department of Homeland Security mission to reduce and eliminate infrastructure vulnerabilities, and to mitigate consequences.

(b) Mission Statement: The mission of InfraGard is to support an information sharing partnership between the private and public sectors for the purpose of protecting the nation's critical infrastructures against attack or failure caused by either foreign or domestic threats, and to

support all FBI investigative programs, including Counterterrorism, Counterintelligence, Criminal and Cyber Crime.

(c) The InfraGard Program classification number is [ ] and the title of the classification is as follows: b3 b7E

INFRAGARD

[ ]-2 KEY TERMS AND ACRONYMS

(1) Critical Infrastructure: The nation's network of interdependent, man-made systems and processes engineered and operated to function collaboratively in order to produce and distribute a continuous flow of essential goods or services at some expected level of service.

(2) Critical Infrastructure Sectors: As of June 1, 2004, the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Branch listed the critical infrastructure sectors as follows:

Agriculture, Food (Meat, Poultry, Egg Products)
Public Health, Healthcare, Food (Other than Meat, Poultry, and Egg Products)
Drinking Water and Water Treatment Systems
Energy (Except Commercial Nuclear Power Facilities)
Banking and Finance
National Monuments and Icons
Defense Industrial Base
Information Technology
Telecommunications
Chemical
Transportation Systems
Emergency Services
Postal and Shipping

(3) InfraGard: An FBI program dedicated to promoting ongoing dialogue and timely communication between the private sector and local, state, federal, and international entities regarding critical infrastructure protection.

(a) Chapter: A partnership which facilitates the exchange of information between the FBI, the InfraGard Member Alliance (IMA), and chapter members, who are the owners and operators of the local and national critical infrastructure. Each chapter addresses concerns of all partners working together for a mutual benefit within the information-sharing context.

(b) Louisiana State University (LSU): Location of InfraGard Program Office.

(c) Member: Individuals with an interest in protecting the nation's infrastructure who have voluntarily applied for membership, been vetted, and been approved as members via the FBI InfraGard application process. Must be U.S. citizen and complete and submit to FBI field office most current version of InfraGard membership application (found at www.infragard.net) so FBI can conduct a security risk assessment.

(d) Membership Application: An online form found at www.infragard.net. Individuals interested in InfraGard membership fill out and submit the form to the field InfraGard coordinator, who oversees its processing. The application serves as a waiver to allow the FBI to conduct records checks, and the coordinator sets those checks to initiate the security risk assessment required for membership.

(e) www.infragard.net: A secure web site which provides members with information about recent intrusions, research related to critical infrastructure protection, and the capability to communicate securely with other members.

(4) IMA: InfraGard Members Alliance, a not-for profit corporation comprised of the elected leaders of the local InfraGard membership. Local IMAs elect members of a national board (INMA) to work directly with a designated FBI InfraGard program manager.

(5) INMA: InfraGard National Membership Alliance, private sector national leadership, elected by local IMAs, represents program's interests of thousands of private sector InfraGard members located throughout U.S. INMA has mission statement and set of bylaws voted on by local delegates representing their chapters at an annual national InfraGard Congress, and in conjunction with the FBI through a Memorandum of Understanding (MOU) between the FBI and the INMA. Local IMA mission statements and bylaws must be consistent with the INMA bylaws and MOU.

(6) Key Resources: As of June 1, 2004, the Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) Branch listed the key resources as follows:

Dams
Government Facilities
Commercial Facilities
Nuclear Reactors, Materials, and Waste

(7) Vetting: The thorough evaluation or examination of InfraGard members.

[redacted]-4 SUMMARY OF LEGAL AUTHORITIES

b3
b7E

The InfraGard Program was created by the FBI to support the nation's critical infrastructure. This program is not mandated by any U.S. laws.

[redacted]-5 POLICIES

[redacted]-5.1 Membership Criteria

(1) The FBI InfraGard Program is engaged with InfraGard membership at both local and national levels to:

(a) Promote ongoing dialogue and timely communication between the private sector and local, state, federal, and international entities regarding critical infrastructure protection. The FBI and InfraGard members are engaged in this cooperative undertaking in recognition that a public/private partnership is of vital importance to our nation's security in preventing attacks against our infrastructure.

(b) Support Department of Homeland Security's mission to reduce and eliminate infrastructure vulnerabilities, and to mitigate consequences.

(2) Membership Suitability: The FBI evaluates applications of all individuals aspiring to be InfraGard members by:

(a) Conducting security risk assessments

(b) Adjudicating results of security risk assessments of applicants

(3) Member Vetting: Vetting, the thorough evaluation or examination of members, is intended to foster trust between the InfraGard members. The InfraGard application process creates a baseline of trust because applicants are willing to share their identities and personal information with the FBI and the FBI approves membership based on the stated criteria. Nevertheless, vetting is a continuous process in InfraGard. It begins with the application process, but continues through the regular attendance of members, the participation of members in activities and projects and the IMA board, and other opportunities. Coordinators should assist members and the public in recognizing the Security Risk Assessment vetting process is not a substitute for a background investigation for a prospective employee.

(4) Membership Recertification: Coordinators ensure members' security risk assessments are reconfirmed on a five-year basis.

(5) Foreign Affiliates:

Individuals who are not U.S. citizens may wish to participate in and support InfraGard while residing in the United States. Such a person may fill out an InfraGard application for a InfraGard Foreign Affiliate membership.

[redacted]-5.2 Member Conduct: Suspension or Removal of Members b3 b7E

(1) Criminal Conduct: Members who are charged with felonies and wish to remain active InfraGard members must notify the coordinator in writing of all charges within 60 days. If a member fails to notify the coordinator within 60 days, that member will be automatically placed in inactive status. Inactive status is a probationary status pending the outcome of any felony charges.

(a) If a member is convicted on a felony charge, the FBI coordinator will advise the FBIHQ InfraGard Program Manager, and the Cyber Division Legal Counsel. FBIHQ will notify the individual that his/her membership has been revoked; and FBIHQ will notify the InfraGard Program Office at Louisiana State University (LSU) and the local IMA of the change in membership status.

(2) Policy Violations: Individuals who sign the InfraGard Membership Application agree to act in a manner consistent with the InfraGard National Bylaws as well as other duly enacted national requirements of InfraGard. Specific concerns include privacy of information, ethical behavior, media or public relations activities, and vendor activities. Member requirements are mandated by the INMA and by IMAs. IMAs' Bylaws may be more restrictive than the INMA. All IMA imposed Bylaws that are more restrictive then those of the INMA must be approved by the FBI.

Violations of FBI-approved policies and requirements should be reported to the IMA and the local InfraGard Coordinator and handled at the lowest level whenever possible. The coordinator can assist the IMA in notifying the violator of the complaint, and should document his actions. If a violation escalates to an official complaint made by the IMA to the INMA, the coordinator will also advise FBIHQ of all details and will make a recommendation independent of the IMA. Recommendations might include a written notice by FBIHQ, suspension of membership, or revocation of membership.

[redacted]-5.3 FBI Field Office Management and InfraGard b3 b7E

While the day-to-day workings of the InfraGard Program are the responsibility of the Agent FBI coordinator, FBI managers

at all levels are encouraged to become involved in InfraGard activities. The Assistant Director in Charge (ADIC) or SAC of a field office is encouraged to meet with InfraGard members at least annually, and should view contact with InfraGard as an opportunity to engage a supportive citizenry in understanding and assisting with the FBI's priorities. ASACs and Supervisory Special Agents (SSAs) responsible for the InfraGard Program, as well as ASACs and SSAs who want to communicate the particular responsibilities of their investigative squads, should utilize the unique, positive relationships developed with the InfraGard members.

Within 30 calendar days of the arrival of a newly assigned ADIC/SAC, ASAC, or SSA within a division, the InfraGard coordinator will brief that person on the InfraGard chapter or chapters affiliated with the division. That briefing will contain a written snapshot of the affiliated chapters, including membership data, infrastructure sectors represented, as well as a summary of chapter activities and accomplishments. Snapshots will be updated and redistributed at least on a six month basis in order to assist the field office management in promoting the InfraGard Program and information sharing.

[ ]5.4 InfraGard Chapter Activities

InfraGard chapter activities may advance local goals and objectives or national goals and objectives. Locally the partners, who make up an InfraGard chapter, may agree to take on a variety of projects with some aimed at serving the InfraGard membership only or some targeting the general community. National initiatives may come out of projects endorsed by FBIHQ and the INMA, or they may grow out of local projects. b3 b7E

Many of the chapters across the country conduct seminars or security days, some every month and some quarterly. The chapter invites speakers to make presentations on a variety of topics related to protecting critical infrastructures. Some chapters have hosted tabletop exercises for their members and for select individuals in the government or significant infrastructure sectors.

[ ]5.5 InfraGard Program Activities

InfraGard Program activities differ from chapter activities as they aim to further FBI objectives. A field office can utilize InfraGard chapter meetings to communicate priorities and investigative interests to the public and InfraGard members about counterterrorism, counterintelligence, and cyber programs. The Assistant in Charge/SAC of a field Office, squad supervisors, WMD coordinators, ANSIR coordinators, all can speak to a supportive audience which is well placed within critical infrastructures.

[redacted]5.6 InfraGard Coordinator

b3
b7E

(1) DUTIES

Each field office will designate at least one Agent InfraGard coordinator to engage the local IMAs and local InfraGard members when making local InfraGard chapter decisions.

While the assigned Agent coordinator must remain cognizant that he/she represents the FBI in a partnership, the coordinator must also recognize he/she is the sole person at the local level who is not a volunteer. The coordinator is a public face for the FBI much like a field office Public Affairs Officer.

The InfraGard coordinator recruits members through presentations and personal meetings, processes membership applications by conducting background investigations, responds to queries and reports from potential members as well as members, and works closely with the IMA(s) and the membership on common goals and objectives.

Typical projects of InfraGard chapters include organizing and hosting quarterly or even monthly security seminars for members or the public, yet several chapters have initiated more ambitious projects. The FBI InfraGard coordinator nourishes the IMAs and local InfraGard chapters toward relative independence, but steadfastly represents the FBI's interests in the partnership while ensuring the local chapter functions.

While the operational duties of keeping a chapter functioning are important, the FBI's critical infrastructure role is focused primarily on threat reduction, by preventing attacks whenever possible and by determining attribution when actual or attempted attacks occur. The FBI InfraGard coordinator must be cognizant that the FBI's involvement in the InfraGard partnership is to that end of meeting the FBI's critical infrastructure responsibilities. The coordinator has the responsibility for educating the InfraGard membership and the public on the FBI's investigative priorities and interests. The coordinator must be a communicator knowledgeable in the FBI's counterterrorism, counterintelligence, and cyber intelligence requirements and linked to the local Field Intelligence Group (FIG) as an integral part of the FBI's intelligence cycle.

(2) TOOLS AND EQUIPMENT

In order to perform the variety of InfraGard Program duties, an InfraGard coordinator requires certain basic business tools and software.

To be responsive to member inquiries on a timely basis, the coordinator must have a cell phone, a laptop, Internet access at his/her desk, standard business software, i.e. Word, Excel, PowerPoint, anti-virus and firewall software. To make presentations, the coordinator needs a projector and a FBI-approved thumb drive.

For presentation materials supplied by FBIHQ and other field offices, coordinators should regularly access the Coordinator's Area at www.infragard.org.

Additional equipment useful to a coordinator is a Personal Digital Assistant (PDA) with contact management software.

(3) SKILLS AND EDUCATIONAL RESPONSIBILITIES

Coordinators require a broad-based knowledge of FBI investigative programs, business skills, and corporate security practices.

Because coordinators should be conversant in counterterrorism, counterintelligence, and cyber matters, it is appropriate for them to take at least the basic courses in those subject areas. Because they are an integral part of the intelligence cycle, it is appropriate for them to be trained in the goals and methods of the intelligence process.

As coordinators work closely with the business sector, they need to develop skills in communication, management, and even marketing. They need to communicate effectively with individuals and groups and to be familiar with presentation software such as PowerPoint. Because they work with an IMA board, they should understand business management and project processes. Keeping InfraGard in the eye of the public and in the hearts and minds of the field office components is also a significant part of a coordinator's duties. A proficiency in marketing is helpful.

Because InfraGard began with an Information Technology (IT) focus, many members are knowledgeable of IT security matters. InfraGard coordinators who speak with those members need to have knowledge of technical terms and issues. The Certified Information Systems Security Professional (CISSP) Certification has become the standard approach to corporate security practices. It categorizes security practices into ten domains, including: 1) Access Control Systems and Methodology; 2) Telecommunications and Networking Security; 3) Security Management Practices; 4) Application and Systems Development Security; 5) Cryptology; 6) Security Architecture and Models; 7) Operations Security; 8) Business Continuity and Disaster Recovery Planning; 9) Law, Investigation and Ethics; and 10) Physical Security. InfraGard coordinators are encouraged to study the ten domains through books and courses. Coordinators

should utilize GETA funds and the FBI University Education Program when possible to keep pace with the standard corporate security practices and technological advances.

[ ]-5.7 Classification

b3
b7E

Beginning in 2003, InfraGard cases are to be investigated under the [ ] classification.

[ ]-5.8 Previous Classification

From 1998 until 2003, InfraGard cases were investigated under the 294 classification.

[ ]-6 ROLES AND FUNCTIONAL RESPONSIBILITIES

(1) Field Offices:

(a) Promote, maintain, and support one or more InfraGard chapters within the field office territory. As a partner the field office will assist with and promote projects proposed by other local chapter partners.

(b) Participate in FBIHQ-initiated projects or in projects initiated by FBIHQ in conjunction with the private sector national leadership known as the InfraGard National Members Alliance (INMA).

(c) Communicate its own investigative priorities (e.g., counterterrorism, counterintelligence, and cyber matters) and interests to the local owners and operators and encourage the reporting of information of interest to the field office.

(d) Query and provide feedback to InfraGard members concerning specific threats or situations.

(e) Survey and initiate collaborate efforts inside and outside InfraGard program.

(f) Recruit citizens who work for companies, organizations, and industries associated with critical infrastructure sectors and key resource categories,

(2) FBI InfraGard Coordinators

(a) Coordinate common goals and objectives with local IMAs and local InfraGard members. Engage local IMAs and members when making chapter decisions.

(b) Organize and host regular (quarterly or monthly) security seminars for members of the public.

(o) Within 30 calendar days of arrival of newly assigned ADIC/SAC, ASAC, or Supervisory Special Agent (SSA) within a division, brief that person on InfraGard chapters affiliated with the division.

(p) Create and update every six months written "snapshot" of division-affiliated chapters, including membership data, infrastructure sectors represented, and a summary of chapter activities and accomplishments.

(q) Instruct FBI employees concerning the InfraGard program.

(r) Ensure members are publicly recognized for time and effort dedicated to enhancing InfraGard's image.

(s) Submit semiannual summary reports to the InfraGard Program Manager at FBIHQ.

(3) ADIC/SAC:

Encouraged to meet with InfraGard members at least annually, and should view contact with InfraGard as an opportunity to engage a supportive citizenry in understanding and assisting with the FBI's priorities.

(4) ASACs and SSAs:

ASACS and SSAs responsible for the InfraGard Program, as well as ASACs and SSAs who want to communicate the particular responsibilities of their investigative squads, should utilize the unique, positive relationships developed with the InfraGard members.

(5) Weapons of Mass Destruction and ANSIR Coordinators:

Communicate responsibilities and concerns to InfraGard members.

(6) FBIHQ

(a) Commensurate to the recommendation of an InfraGard coordinator, denies InfraGard membership applications when appropriate and provides written notification of denial to applicant and respective InfraGard coordinator.

(b) Guided by precedent and with the guidance of the Office of the General Counsel, as needed, approves or denies membership applications in cases when derogatory information is uncovered.

(c) Notifies individuals of revocation of their memberships.

(d) Notifies InfraGard Program Office at Louisiana State University (LSU) and local IMAs of any changes in membership status.

(e) Participates in regular regional working group coordinator conference call to determine goals, objectives, and needs.

(f) Assists InfraGard coordinators with chapter-specific projects and reports.

(g) Tracks membership growth and sector representation statistics.

(h) Reviews InfraGard Chapter semiannual reports and provides feedback as needed.

(i) Conducts briefings of SACs and other executive management regarding field office participation and accomplishment with respect to InfraGard.

(j) Works with the INMA to plan and conduct a national Congress and Conference event annually.

(k) Regularly meets with members of the INMA to determine and fulfill national level InfraGard needs.

(l) Regularly works with other Units and Divisions to advance the goals of InfraGard.

(m) Conducts liaison and other appropriate activities with Federal, State, and local law enforcement agencies with an interest in goals parallel to InfraGard.

(n) Plans and conducts InfraGard coordinator training annually or as deemed necessary.

(o) Plans and hosts an InfraGard Technology Exposition at FBIHQ annually.

(p) Works with LSU and other technology providers to establish good technology and database resources for InfraGard.

(7) InfraGard Members

(a) Individuals interested in applying for InfraGard membership must access the InfraGard national

electronic application at www.infragard.net or through links on local InfraGard chapter websites.

(b) Must notify InfraGard coordinator within 60 days if they are charged with a felony and wish to remain an active InfraGard member.

(c) Must notify InfraGard coordinator if they relocate and wish to change chapter affiliations. Must provide updated contact information.

(d) Must notify InfraGard coordinator when no longer interested in membership.

(8) InfraGard Chapters

(a) Designate a membership coordinator from the private sector who is responsible for the chapter membership list.

(b) May require annual reaffirmation of membership or a verification of current member contact information.

(9) National Program Office at LSU

(a) Process all InfraGard membership applications.

(b) Assist the FBI Program Office with the organization of training conferences, including creation of training documentation and presentations.

(c) Moderate national program Listserv to include approve/reject subscriptions and postings.

(d) Travel to InfraGard conferences and meetings to train membership on latest features of the InfraGard Program.

(e) Serves as the liaison for the FBI InfraGard Program Office to FBI Field Offices and national membership base of over 11,000 to determine program needs, practical implementation of program requirements, and promotion of InfraGard membership on a national level.

(f) Main point of contact for National Program.

(g) Coordinate daily with FBI Special Agent Chapter Coordinators via email, phone, and fax in regards to database functionality, chapter Listserv creation and utilization, membership status reports, chapter membership statistics, membership verification, membership discrepancies, application processes, membership approval processes, VPN integration,

coordinator access permissions, new coordinator additions, and coordinator removals.

(h) Format and upload daily html content for websites including news articles, newsletters, daily reports, and announcements as well as special documents/materials such as DHS, FBIHQ and IEB information, announcements, alerts, and advisories.

(i) Create/maintain chapter web pages on public site.

(j) Recommend, create and test new processes for content and membership.

(k) Administer governmental 508 compliancy issues concerning websites.

(l) Create, design, edit printed materials including: welcome packet documents, folders, informational brochure and CD-ROMs.

(m) Single point of contact, 24 hours a day, for the InfraGard program.

(n) Assist members in InfraGard account set-up, connectivity, and troubleshooting.

(o) Assist with FBI surveys.

(p) Provide engineering and technical support for the following activities: estimating resources, developing project schedules, planning user-related networks and systems, developing appropriate technical solutions to network management security requirements, and developing alternative technical approaches to current operations.

(q) Provide the following program services and support activities: provide liaison support, provide problem resolution, provide feasibility analysis, develop concept of operations, provide operational analysis, provide studies for problem resolutions, estimate resources and coordinate user related information.

(r) Provide/support system life cycle development activities associated with the current InfraGard system and associated future relocation of the InfraGard system at a primary location and at a disaster recovery location.

(s) Perform computer system and database and data entry administration activities.

(t) Provide Program Management Reviews (PMR) upon request.

[redacted]-7 RECORDKEEPING REQUIREMENTS b3 b7E

There are no disposition requirements for the [redacted] classification.

[redacted]-8 PROCEDURES AND PROCESSES

[redacted]-8.1 Maintaining a [redacted] Control File

Each field office is to maintain a [redacted] control file as a repository for information concerning the local InfraGard chapter or chapters. Many field offices have found it useful to establish subfiles to document the following categories:

(1) HQ administrative instructions

(2) Membership applications

(3) Intelligence reporting

(4) Expenses

(5) Accomplishments

[redacted]-8.2 Membership Processes and Procedures b3 b7E

(1) Potential Members

(a) Individuals interested in applying for InfraGard membership must access the InfraGard national electronic application at www.infragard.net or through links on local InfraGard chapter websites.

(b) Interested individuals must complete the application online, print it out, and mail it to the appropriate field office InfraGard Coordinator. The applicant may choose the state and chapter for membership affiliation on the application. The application automatically provides the mailing address of the field office affiliated with that chapter.

(2) Coordinator - Processing Application/Security Risk Assessment and handling Membership Records

(a) Coordinator's Actions upon Receipt of Application:

3) NCIC

4) Local criminal history records

b. Records checks for foreign affiliate applications could also include the following:

1) Interpol query

2) INS check

3) Processing of fingerprints

4) Checks required for a U.S. citizen applicant

c. Coordinator follows up with leads on record checks which identify references to or main files on the applicant in other field offices when details are not accessible electronically. The coordinator will set a lead in the field office InfraGard [redacted] file to the InfraGard Coordinator in the appropriate field office.

d. The coordinator reviews and documents the results of the records checks. b3 b7E

4. Coordinator's Actions when Results of Leads/Checks produce NO Derogatory Information

a. If responses to leads and results of records checks produce no information which precludes approval, coordinator recommends approval via an FD-542 to his/her field office [redacted] file. (The FD-542 is a cover communication for the original application, which must be signed by the ADIC/SAC or his designee.) Generally, multiple applications may be consolidated on an FD-542. This communication should include the Name, Date of Birth, Social Security Number and Company Name of each approved member. This communication also serves to claim the accomplishment of developing InfraGard members.

b. In the coordinator's InfraGard working file, place a copy of the front page of the application to be used as a quick reference guide.

c. Notifies National Program Office at LSU of approval of InfraGard applicant by accessing the national InfraGard database available to coordinator at InfraGard web site, www.infragard.org:

(c) Ensures FBI's investigative priorities concerning preventing attacks and determining attribution when attacks occur are communicated to InfraGard members.

(d) Must be knowledgeable and able to communicate intelligence requirements of FBI's counterterrorism, counterintelligence, and cyber programs and linked to local Field Intelligence Group (FIG) as an integral part of the FBI's intelligence cycle.

(e) Recruit members through presentations and personal meetings.

(f) Respond to queries and reports from members and potential members.

(g) Identify and contact physical security, cyber security, and sector leaders in chapter area. Work with field office security officer to obtain security clearances for these individuals on a case-by-case basis to share sensitive information as needed.

(h) Process membership applications by conducting background investigations with security risk assessments. InfraGard coordinators and field offices are to report any applications with derogatory information to FBIHQ InfraGard Program Managers for consideration and final determination. InfraGard coordinators and field offices are not authorized to independently deny InfraGard applications.

(i) Assess and monitor potential risks to other InfraGard members and FBI regarding applicants' indices results and respond to investigative opportunities.

(j) Reconfirm security risk assessments of members on a five-year basis.

(k) Contact members to determine if clearances are being reissued.

(l) Advise FBIHQ InfraGard Program Manager and the Cyber Division Legal Counsel when members report they've been charged with felonies.

(m) Assist IMA and document complaints regarding members' violations of FBI InfraGard policies.

(n) Advise FBIHQ of all details and make recommendations, independent of the IMA, when members' policy violations escalate to official complaints.

1) The coordinator accesses that site via a Virtual Private Network (VPN) [redacted] b7E

2) The coordinator follows the link to the Coordinator's Area (www.infragard.org), and then to the database, which he/she accesses via the same user ID and password needed to access the site. The link labeled "Coordinator's Queue" leads to a database listing of all applications received by LSU where approval is pending for respective members of each chapter.

3) The coordinator indicates approval by clicking on the "Approve" button.

4) The coordinator will advise the private sector membership coordinator (previously designated by the local InfraGard Chapter) of membership approvals if access to the national database is unavailable to the membership coordinator.

5. Coordinator's Actions when Results of Leads/Checks Produce Derogatory Information:

a. When derogatory information is developed which precludes membership approval, the application will be denied by FBIHQ.

b. The coordinator will provide the details of the derogatory information via an FD-542 to the InfraGard Program Manager and the Legal Counsel in the Cyber Division and provide a copy to the field office Chief Division Counsel.

c. In addition to citing the derogatory information, the coordinator will document in the FD 542 the local field office accomplishment of processing the application and will pass on further processing to FBIHQ. The coordinator then accesses the national InfraGard Program Office database via the Coordinator's Queue and indicates the member is not approved.

6. Coordinator's Actions when Results of Leads/Checks Produce Derogatory Information with Mitigating Circumstances:

a. Local field office may recommend approval to FBIHQ and inform the Program Manager and the Assistant General Counsel of the details.

b. The field office will submit an FD-542 to FBIHQ providing details of the derogatory information,

summarizing the mitigating circumstances, and documenting the processing of the application.

c. The coordinator then accesses the InfraGard database via the Coordinator's Queue and approves the applicant's membership.

d. The Coordinator will advise the applicant of his/her approval via a welcoming letter from the ADIC/SAC of the local field office.

(d) Coordinator's Establishing of Application Tracking System:

Because of the high volume of InfraGard applications processed over time, the variety of issues which may arise over application, and various other membership issues, coordinators are strongly encouraged to develop and maintain a tracking system for applications.

(e) Coordinator's Duties regarding Membership Changes (Relocations, Discontinuance of Membership, etc.)

1. Ensures members' information is updated in or removed from the InfraGard national database and documented in local field office file.

2. Prepares ECs to appropriate field offices when members relocate and wish to change chapter affiliations. EC should contain member's new contact information.

3. Advises national InfraGard Program Office and local InfraGard membership coordinators of membership changes.

(f) Coordinators distribute color-coded membership cards to members at annual InfraGard Congress.

(g) Coordinator's Duties concerning the Member Recertification Process

1. The InfraGard Coordinator ensures security risk assessments are reconfirmed on a five-year basis. Six months prior to the fifth anniversary of membership approval, the InfraGard Coordinator will request the member to resubmit an application for review by the field office.

2. If a security clearance was used in lieu of the initial application criminal records checks, the expiration date of the clearance will dictate the date of the recertification.

(3) ADIC/SAC .

(a) Signs application signature page for approved applicants

(4) FBIHQ

(a) Deny application

(b) Approve application when derogatory information found on applicant

(c) Deny application when derogatory information found on applicant

(5) National Program Office at LSU:

(a) Enters data from photocopies of member applicants into national InfraGard database.

(b) After a new member is approved by the InfraGard coordinator and is listed in the database of members affiliated with his/her particular InfraGard chapter, the InfraGard Program Office at LSU sends a new member a packet of information, an InfraGard membership card, and VPN client software.

[redacted]8.3 Public Relations and FBI Education Processes b3 b7E

Each InfraGard coordinator is a public face for the FBI and InfraGard both locally and nationally. Coordinators are often contacted to make presentations, participate in panel discussions, talk to the media, and to respond to queries from potential members. All these are opportunities to communicate the interests and priorities of the FBI, but should be processed through the appropriate channels.

(1) Making Presentations

Requests for presentations must be made via letter or E-mail and the actual presentations documented on FD-542s for the Cyber Division and on a FD-772 for the local field office Outreach Coordinator. Coordinators should not wait to be asked to present, but should target and contact specific companies, organizations, and industry groups with offers to make InfraGard presentations. Within the FBI field office, the coordinator should work closely with and make presentations to the Citizens Academy and the local National Academy Alumni organization.

(2) Media Interviews

1. Reviews the document to ensure it was completed correctly.

2. Within a week, the coordinator should mail a photocopy of the application via cover letter to the InfraGard Program Office at Louisiana State University (LSU), which enters data from the application into a national database. LSU will automatically send an E-mail to the applicant acknowledging the receipt of the application.

(b) Coordinator's Actions when Applications are Incorrect or Incomplete:

Applications that were completed by hand or filled out incorrectly or incompletely will NOT be accepted by the InfraGard Program Office at LSU. In such cases the Agent will notify the applicant that a new application must be completed and submitted.

(c) Coordinator's Processing of Correctly Submitted Applications:

1. Either begin the security risk assessment or verify an applicant's current security clearance to be accepted in lieu of the risk assessment.

2. If verifying applicant's current security clearance:

a. InfraGard coordinator will contact the applicant's security officer in person or by telephone and request verification of the applicant's clearance.

b. The coordinator will ask the security officer to identify the clearance and the expiration date of that clearance, and will document that information to the InfraGard file.

3. In cases where the InfraGard coordinator conducts a full security risk assessment:

a. Because the application serves as a waiver to allow the FBI to conduct records checks, the coordinator sets those checks to initiate the security risk assessment required for membership. The coordinator checks the following records:

1) FBI indices

2) Department of Motor Vehicles

(a) General member inquiries

(b) Industry or business sector, subject matter experts, and individual inquiries.

(2) The information sensitivity levels may be described as:

(a) open to the public

(b) SENSITIVE, unclassified, including law enforcement, industry sector, member sensitive, and NOFORN.

(3) The sensitivity levels will dictate the method of contact. Possible methods of contact may be:

(a) E-mail

(b) IRC Chat

(c) Telephone

(d) Encrypted and authenticated e-mail

(e) In person

[redacted]-8.7 Communications and Reports Processes

(1) The InfraGard coordinator utilizes a variety of communications tools and technology to accomplish his/her goals and objectives, including Internet e-mail, pager, telephone, and fax. Documentation may take a variety of forms, but should be retrievable, and should be placed in the field office InfraGard file. b3 b7E

(2) Communications and reports document the:

(a) The InfraGard Database

(b) Internet and Intranet e-mail

(c) Semiannual Report to FBIHQ

The Semiannual Report needs to be uploaded to ACS.

[redacted]-8.7.1 Membership Application Process

As part of the application process coordinators will use the application and FD-542s.

(1) The original applications will be attached to a FD-542 which will include the Name, Date of Birth, Social

Often the InfraGard coordinator has opportunities for print, radio, and television interviews. All media contacts must be coordinated with the field office Public Affairs Officer (PAO). While the PAO may wish to be present during an interview, often coordinators are authorized by the ADIC/SAC to do such interviews without the PAO. Coordinating with the PAO can also be useful for announcing InfraGard events and activities via a press release or statement by the ADIC/SAC to the local media.

(3) FBI Instruction

In addition to educating people outside the FBI about InfraGard, the InfraGard coordinator should be educating the FBI about the InfraGard Program and its ability to assist various FBI squads in meeting their objectives. The InfraGard coordinator should be a speaker at his/her field office's all-employees conference, should speak at supervisors' meetings, and should speak directly to substantive squads.

(4) Internet Websites

Each InfraGard chapter should maintain its own Internet website and have a presence on the local FBI field office's website. The FBI, its priorities and interests should appear on the local InfraGard web site, and the InfraGard Program and its associated local chapter or chapters should be featured on the local FBI field office's website. Information to be included on the sites should be who, how, and about what to contact the FBI.

Information to be placed on the website is up to the individual chapters and field offices, but it is imperative that content be informative and updated on a regular and timely basis.

[redacted]-8.4 Recognition of Members b3 b7E

It is important for the coordinator to recognize publicly members who have dedicated time and effort to enhancing the InfraGard image. One way to do so is through annual awards recognition for citizens such as the Director's Certificate.

[redacted]-8.5 Intelligence/Investigative Processes

(1) Coordinate with Field Intelligence Group (FIG):

(a) The InfraGard coordinator will provide access to local InfraGard membership for the FIG and field office substantive squads. The InfraGard Coordinator should work with the FIG to establish and maintain a database of member companies

and organizations, which Agents can query for contacts and information.

(b) By coordinating with the FIG on current intelligence requirements, the InfraGard coordinator can develop tasking for specific InfraGard members or infrastructure sectors. InfraGard members can be queried as subject matter experts or members of a business or a business sector to assist with investigative matters.

(c) Often InfraGard members provide unsolicited information, and it is the role of the coordinator to direct that information to the FIG and substantive investigative squad.

(2) Documenting Information:

It is important for the InfraGard coordinator to document all significant incoming information and its dissemination. Documentation may be via FBI Intranet E-mail serialized to the InfraGard file, or may be an EC or FD-542 sent to the FIG, appropriate substantive squads, and the file. More significant information which may need to be disseminated by the FIG in an Investigative Intelligence Report (IIR), should be written as an EC or FD-542 and utilize the following lead paragraph.

> "An FBI InfraGard member provided the information below. Dissemination of this information should identify the source of information as an FBI InfraGard member but should not identify the individual by name."

(3) Membership Feedback:

The coordinator should look for opportunities to provide feedback to InfraGard members regarding their information provided to assist with FBI investigations. As it is important for the InfraGard member to feel he/she has contributed to the FBI mission, the coordinator must provide members some feedback information. The feedback can take many forms and should be presented generally to the InfraGard membership using nonspecific statistics. For example, the InfraGard coordinator could publish local statistics on the number of member-initiated reports received by the local field office with their results, identifying the number of cases opened and the number of disseminations to the intelligence community.

[redacted]8.6 FBI Intelligence Inquiries Process b3 b7E

(1) The process of querying members may be through several different methods, including:

Security Number and Company Name of the applicants. The FD-542 will be serialized to the InfraGard file maintained at the field office level.

(2) A copy of the front page of the application will be maintained in the coordinator's InfraGard working file for quick reference.

(3) Member's Name, Date of Birth, Social Security Number and Company Name should be indexed in UNI and accessible via ACS.

[redacted]-8.7.2 InfraGard National Database b3 b7E

InfraGard coordinators will use the InfraGard National Database as the official documentation of membership data. The secure database is available to all coordinators and FBIHQ at www.infragard.org. Coordinators use the database to document when an applicant is approved, and FBIHQ utilizes the membership numbers documented in the national database to describe accurately program membership statistics. Coordinators are to ensure that field office data accurately reflects local field office numbers.

[redacted]-8.7.3 E-mail Communications b3 b7E

Pertinent InfraGard E-mail will be retained and placed into the [redacted] InfraGard field office file. The format may be on paper or burned to a CD.

[redacted]-8.7.4 Semiannual Summary Reports

A report summarizing InfraGard activities is to be submitted for the first six-month period and for the second six-month period of the fiscal year. Within 30 days following the end of each reporting period, each field office is required to provide the summary report to the InfraGard Program Manager at FBIHQ. See EC titled, "SEMIANNUAL REPORT; INFRAGARD PROGRAM," dated May 28, 2004. The summary will include the following information:

(1) Membership statistics, including total number of members, number of members processed during the period, number of members approved during the period, number of members pending, number of members denied during the period.

(2) Summary of information reports received from InfraGard members, from InfraGard member Subject Matter Experts, from non-InfraGard members, with the number of disseminations, and the number of cases opened by the field office.

(3) A summary of InfraGard presentations made.

(4) A narrative summary of InfraGard activities, initiatives, and other significant accomplishments.

MIOG, Part 1, Section 294, should be changed as follows:

SECTION 294. INFRASTRUCTURE PROTECTION (IP)
(RECLASSIFIED AS [ ]
CLASSIFICATION
--SEE MIOG, PART 1, SECTION [ ].)

294-1 INFRASTRUCTURE PROTECTION

This classification was discontinued in fiscal year 2003 and replaced with classification [ ] InfraGard. See MIOG, Part 1, Section [ ] for instructions.) b3 b7E

INDEXING

The heading "InfraGard, I, [ ]" should be placed in the MIOG index.

SAC MEMORANDUM

SAC Memorandum will be sent out on the InfraGard Policies and Procedures.

LEAD(s):

Set Lead 1: (Action)

RECORDS MANAGEMENT

AT WASHINGTON, DC

Upon approval of manual changes, this EC should be forwarded to Manuals Desk, Records Management Division, for handling.

1 - [redacted]
1 - Manuals Desk, Rm. 6094

♦♦

b6
b7C

C:\Documents and Settings\[redacted]Desktop\MIOG.wpd

SAMPLE

Precedence: ROUTINE Date: 10/04/2005

To: Cyber Attn: Public/Private Alliance Unit
FBIHQ, Room 5842

From: [your division]
[your squad designation]
Contact: [name of InfraGard Coordinator, your phone #]

Approved By: [SSA over InfraGard's name]

Drafted By: [whoever prepares the EC]:abc

Case ID #: [FIELD OFFICE FILE #] ~~(Pending)~~ [redacted] b3 b7E

Title: SEMIANNUAL REPORT;
INFRAGARD PROGRAM;
[YOUR FIELD OFFICE];
[YOUR CHAPTER'S NAME]

Synopsis: This document is the [Your] Division's Semiannual InfraGard Program Report for the period [either 4/01/200? to 9/30/200? or 10/01/200? to 3/31/200?.]

Details:

I. INFRAGARD PROGRAM INFORMATION

A. Personnel

1) Supervisory Special Agent: [List in chronological order, the SSAs who have supervised the InfraGard Program during the reporting period and how long they had the program.

2) InfraGard Coordinator: [list all coordinators during the six month period, along with the following information for each.]

a) Coordinator since: [date]

b) Percentage of time devoted to InfraGard:[your best estimate]

c) List other duties assigned: [i.e. CART, approximately x number cases, case agent on Group I UCO, etc.]

d) Coordinator Background:

1. Number of years in the FBI.
2. Previous programs worked.
3. Previous significant liaison experience

3) Assistant Coordinator: [explain if you have an official Assistant Coordinator, if you asked for and were denied one, if your request is pending, if you have the part time assistance of other agents who are unofficial assistant coordinators. No need to list sub-questions a), b),c) or d) that is required under 1 above.]

4) Other Program Support: [Describe any support personnel assigned to support the InfraGard Program on a consistent basis.]

B. Program Activities

1) List, in date order, all meetings your chapter has held, sponsored, or actively participated in during the reporting period: [list date, name of activity and whether it was your event or you joined another coordinating entity as a participant.

2) Briefly describe your program/chapter's two most significant events and/or accomplishments during the reporting period: [Describe the purpose or theme of the event, who participated, how many attendees, methods of publicizing the event, who the most notable persons in attendance were, and who from your division management attended and in what capacity. This should take 1-3 paragraphs, depending on the size of the event. If you have more than two, list as many as you feel were noteworthy. Remember, it need not be an event. An accomplishment may relate to creating a chapter board or holding elections, or settling some chapter difficulty, or managing the transition of your chapter to all secure membership. If you had less than two, explain why (i.e. your chapter lacks available volunteers to assist and you lacked time/resources to do more; you were in trial or on TDY; there were other events taking the stage that would have competed with an InfraGard event; etc.]

3) Please answer the following regarding your routine chapter meetings:

a) How often held?

b) Do you ever have "closed" (secure members only) meetings?

c) TURK Burn & Statistical Accomplishments

1) What is your division's TURK hours for [redacted] matters for the period ending [either 3/31/200? or 9/30/200?]? [Ask your supervisor or one of the executive assistants who can run this report for you.] b3 b7E

2) What statistical accomplishments have you claimed on behalf of the InfraGard Program during the reporting period?

FD-542 InfraGard Member Developed _____
FD-542 InfraGard Information Disseminated/Referenced_____
FD-542 InfraGard Presentation Conducted #_____
FD-542 InfraGard Case Initiated from Information Provided by an InfraGard member_____

If added to the FD-542, how many instances would you have reported for:
Positive Intelligence Reported by an InfraGard member_____

[There is a differentiation between Cases Initiated and Positive Intelligence Reported to enable us to distinguish statistically between information good enough that it resulted in a case opened and positive intelligence that was put in the classification's "zero" file, and may or may not have been forwarded to another agency.

3) List, by case number, the cases opened based on information provided by an InfraGard member. Include all program classifications (i.e. [redacted] 196, [redacted] etc.). Follow each with a brief description of the referral circumstances, the nature of the information, and whether investigation is on-going or resolved. [The number of items in this answer should match the number of FD-542 stats under "Case Initiated in 2 above. We're not looking for zero file items.] b3 b7E

4) List instances where InfraGard members have provided significant information that enhanced on-going investigations. [Include instances across all investigative programs, not just cyber crime.]

5) Describe the involvement of investigative programs other than Cyber with InfraGard in your Division. [Examples might be lists of contacts other squads have provided for recruiting into InfraGard (i.e. Banking community as they're not only a WCC contact, but members of the Banking and Finance Critical Infrastructure Sector.); or presentations by agents to your InfraGard chapters to alert them what to be on the lookout for and report to the FBI; or any joint collaboration with your office's Domain program (see your counterintelligence squad members), WMD coordinator, or Domestic Preparedness agents.

6) List any sources opened that can be credited to the InfraGard program, either directly or indirectly. [Use symbol numbers only. Include those opened under every program, not just Cyber.]

7) List any instances where information provided by an InfraGard member was shared with another law enforcement or public sector entity (including your State Homeland Security or the federal Department of Homeland Security.) How do you document this?

D. Management Support

1. ADICs Support [Only applies to LA, NY, WHO] [How has the ADICS shown his/her personal support for InfraGard during the reporting period?]

2. SAC Support [How has the SAC shown his/her personal support for InfraGard during the reporting period?]

3. ASAC Support [How has the ASAC shown his/her personal support for InfraGard during the reporting period?]

II. CHAPTER INFORMATION

1. Of your total members, how many are:
a) private sector
b) public sector - not law enforcement
c) public sector - law enforcement (state, local, and federal)

2. Does your chapter have a public website? If yes, please answer the following:

a) Provide url. www._____
b) Who is the Webmaster for it?_____[FBI person or a chapter member]
c) How often (approximately) is it checked for needed updates? [Please do not put "as needed". We are trying to document how well chapters and/or coordinators are able to managing their own public sites.]
.d) Did LSU assist you in setting up your chapter's site? If not, did you know they could do so?

B. Chapter Management

1. Do you have a chapter board? If not, describe your efforts to form one. If none, what are the mitigating circumstances.

2. If yes, describe its composition by name, occupation, and duration of service.

3. Characterize the quality and quantity of participation of board members in helping you run and provide events for your chapter.

4. What is the most frequent complaint you hear from your board members?

5. What is the most significant complaint you have about your board members?

6. How often does your board meet?

7. How often does your chapter have elections for board members and is this in compliance with your by-laws?

III. CRITIQUE OF HQ PROGRAM MANAGEMENT

A. Training: [Please comment on all aspects of training received during the reporting period. If none, because no conferences were held, comment on whether or not HQ personnel adequately compensated with individual help with your questions. While we like to hear good feedback, we learn how to improve through your criticism.]

B. Guidance: [Are you satisfied with the number and level of detail in the policy and procedure ECs promulgated by HQ? What areas of the program do you need guidance on? List as many as you like.]

C. Facilitation: [What do you need HQ to facilitate for your InfraGard Program that you are not seeing currently? List as many as you like.]

D. Open Comment: [For any comments on any aspects of HQ program management that is not covered above.]

♦♦

b6
b7C

STANDARDIZED RECORD CHECKS FOR INFRAGARD APPLICANTS

Applicant Name. _____
DOB: _____
SSN: _____

BACKGROUND CHECKS

Contractor Exclusion
List of Parties Excluded from Federal Procurement and Non-procurement Programs - http://www.arnet.gov/epls/

CRIMINAL HISTORY

Conducted by:	
Date:	

DMV CHECK

Conducted by:	
Date:	

INDICES/ACS CHECK

Conducted by:	
Date:	

NCIC

Conducted by:	
Date.	

FIELD OFFICE APPROVAL

Field Office Approval (by SSA or Above):	
Date of Approval:	

May 26, 2005

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE Date: 03/13/2006

To: All Field Offices Attn: ADICs
SACs
InfraGard Supervisors
InfraGard Coordinators
FBIHQ, Manuals Desk

From: Cyber
Information Sharing and Analysis Section
Public/Private Alliance Unit (PPAU)
Contact: UC [redacted]

Approved By: [redacted] b6 b7C b7E

Drafted By: [redacted]

Case ID #: [redacted] b3 b7E

Title: PUBLIC/PRIVATE ALLIANCE UNIT;
INFRAGARD PROGRAM UPDATE

Synopsis: To communicate the mission of the PPAU; provide background information on the InfraGard Program; outline the PPAU organizational structure; provide an update on PPAU initiatives; provide an update on the InfraGard applicant process; provide an update on the Clientless Virtual Private Network (C-VPN) implementation; provide an update on PPAU staffing; and set forth a schedule for PPAU communications to the field.

Enclosure(s): Copy of PPAU SSA and Management and Program Analyst InfraGard Region Assignments Matrix.

Details:

Public/Private Alliance Unit Mission

The Public/Private Alliance Unit (PPAU)is within the Cyber Division, Information Sharing and Analysis Section (ISAS). The mission of the PPAU is to develop partnerships between the FBI and private sector, academia and other public entities, and to support the Cyber Division National

Strategy and the FBI's Counterterrorism, Counterintelligence, and other priority investigative programs.

The National InfraGard Program is at the forefront of the PPAU's efforts. InfraGard is an FBI program that began in the FBI's Cleveland Office in 1996. In 1998, InfraGard was assigned a Program Manager from FBI Headquarters and has since developed a relationship of trust and credibility in the exchange of information concerning various terrorism, intelligence, criminal, and security matters. InfraGard's information sharing and analysis effort serves the interests and combines the knowledge base of a wide range of nearly 14,000 members who represent all thirteen critical infrastructures and four key resources.

PPAU Organizational Structure

As InfraGard Coordinators are aware, there are currently six InfraGard Regions within the United States: Northeastern, Southeastern, Midwestern, Western, Southwestern, and Pacific. During late FY 2005, in an effort to improve responsiveness and provide more effective support to InfraGard Coordinators, PPAU Supervisory Special Agents (SSAs) and Management Program Analysts (PAs) were assigned regional responsibilities. As a result, each SSA and MPA assigned to an InfraGard Region was assigned responsibility for all activities associated with that region. These activities include assistance/guidance with applicant processing, on-site inspections, review of Semiannual Program Reviews, assistance with the development of private sector initiatives, and participation, when appropriate, in InfraGard Chapter events. Please note, effective 03/01/2006, SSA regional responsibilities were realigned to reflect an additional SSA in the PPAU. Please refer to the enclosure entitled "SSA and Management and Program Analyst InfraGard Region Assignments" for details.

PPAU Initiatives

Special Interest Groups (SIGs):

InfraGard currently has implemented two SIGs, Food/Agriculture InfraGard and Chemical InfraGard. Both SIGs are collaborative projects with the Counterterrorism Division (CTD) and Louisiana State University (LSU).

Chemical InfraGard was implemented on 12/17/2005 and is accessible via InfraGard.org. This secure SIG is for current and new InfraGard members who work in or are associated with the Chemical Sector. Members will be able to exchange information related to the chemical sector, access reference material and a Frequently Asked Questions (FAQ) section, a Feedback Section, and receive intelligence pertinent to the Chemical Sector. Content for Chemical InfraGard is updated weekly. All content submitted is approved by CTD, WMDCU, as well as PPAU. Content may be submitted to chemicalcontent@infragard.org. Presently, Chemical InfraGard has over 60 members.

Food and Agriculture InfraGard was implemented on 03/01/2006 and is accessible via InfraGard.org. This secure SIG is for current and new InfraGard members who work in or are associated with the Food and Agriculture sector. Members of this SIG will have access to similar capabilities as those enumerated above for the Chemical Sector. Content for Food/Agriculture InfraGard is expected to be updated weekly. All content submitted is approved by CTD, WMDCU, as well as PPAU. Content may be submitted to food-agcontent@infragard.org.

Intelligence Initiative:

PPAU has made significant advances in the dissemination of intelligence products to the InfraGard Membership. During Fiscal Year (FY) 2005, as a result of discussions with the Directorate of Intelligence (DI) and Office of General Counsel (OGC), InfraGard was listed on page two of the FBI Intelligence Product Abstract and "Admonishments" (what members may do with an intelligence product) were posted on the secure web. Consequently, the PPAU disseminated three Intelligence Assessments, 50 Intelligence Bulletins, and six Intelligence Information Reports to the InfraGard membership during FY 2005. To date, in FY 2006, the PPAU disseminated ten Intelligence Bulletins and one Intelligence Assessment.

During the last few months, questions have arisen from field personnel and FBI Headquarters divisions regarding the classification of intelligence suitable for dissemination to the InfraGard membership. Please note that in accordance with discussions with the Directorate of Intelligence and Office of General Counsel, and with the permission of the originator of the intelligence product,

the InfraGard membership is eligible to receive the following categories of information: Unclassified, Unclassified/Law Enforcement Sensitive (U/LES), Unclassified/For Official Use Only (U/FOUO) and Sensitive But Unclassified (SBU). These intelligence products may include Intelligence Information Reports (IIRs), Intelligence Bulletins (IBs), and Intelligence Assessments (IAs).

The Intelligence Initiative is on-going and PPAU will continue to work closely with the DI regarding the dissemination of intelligence. The work accomplished with DI has also allowed the PPAU to seek approbation of the InfraGard Program and its secure VPN to allow for the posting of Department of Homeland Security Unclassified documents. Finally, PPAU is making every effort to ensure the Counterterrorism, Counterintelligence, and Criminal Divisions include InfraGard in all pertinent intelligence disseminations.

InfraGard Applicant Process

As everyone is aware, the integrity of the InfraGard Program is based on its membership. Therefore, it is imperative that InfraGard Coordinators, as well as PPAU SSAs, make every effort to ensure that only well intentioned citizens become InfraGard members. As a result, if derogatory information concerning an applicant is uncovered, the InfraGard Coordinator should make every effort to gather the pertinent details and document them in an EC to the appropriate SSA within PPAU. Additionally, the EC should contain an accept or reject recommendation for the potential member. The EC will then be reviewed by the PPAU SSA, UC, and if appropriate, the Office of General Counsel (OGC) attorney assigned to Cyber Division for final adjudication. Once the matter is adjudicated, an EC from PPAU to the field division will be disseminated. Please note, InfraGard Coordinators are encouraged to contact the SSA responsible for his/her region with any questions which may arise during the applicant process and prior to sending an EC.

Clientless, Virtual Private Network (SSL-VPN)

As many of you are aware, throughout the history of the InfraGard Program there have been objections to the current Virtual Private Network (VPN). Presently,

Public/Private Alliance Unit

InfraGard Program

June 2007

b6
b7C

~~(Not for Public Release: FBI only)~~

InfraGard Briefing Book

(June 2007)

- **Personnel**
  - UC [redacted]
  - SSA (TDY) [redacted] (Transfer 7/07)
    - Northeastern
  - SSA (TDY) [redacted] (Transfer 9/07)
    - Southeastern/Pacific
  - SSA (TDY) [redacted] (Transfer 9/07)
    - Southwestern/Western
  - SSA [redacted]
    - Midwestern
  - MPA [redacted]

- **Statistics**
  (InfraGard statistical spreadsheets are provided to each Field Office)
  - Cases Initiated
    - FY 2007 (first half) - 44 total (10/01/2006 - 03/31/2007 for FY07)
    - FY 2006 - 103 total
    - FY 2005 - 65 total
    - **Aggregate - 212**
  - Cases Enhanced
    - FY 2007 (first half) - 85 total (10/01/2006 - 03/31/2007 for FY07)
    - FY 2006 - 140 total
    - FY 2005 - 60 total
    - **Aggregate - 285**
  - Intelligence Products
    - FY2007 (first half) - 139 total (10/01/2006 - 06/19/2007 for FY07)
    - FY2006 - 145 total
    - FY2005 - 60 total
    - **Aggregate - 344**

~~(Not for Public Release: FBI only)~~

b3
b7E

Leading Initiatives/Projects

- InfraGard System Upgrade (Detailing All Field Office EC forthcoming)
  - Online Member Application/Membership Profile
  - System Security Policies
    - Re-vetting options
    - Secure web access requirement policy ("180-day Rule")

- Semi Annual Report (SAR)
  - Coordinating with the Louisiana State University program office to create a statistical database and to eventually automate the SAR input process

- Request For Investigative Information
  - Formulating a policy EC whereby the membership can be queried for information to aid investigations and intelligence gathering

- FD-515
  - Implemented with ongoing usage education effort

- SAC Metrics
  - InfraGard incorporated

- Secure Video Teleconference
  - September 19, 2007, InfraGard National Members Alliance (INMA) Congress as detailed in an All Field Office EC

- INMA Statement of Work
  - Contract enacted with the INMA for an Executive Director position and to enhance the program for both the INMA and FBI

- Coordinator/Field Office support
  - Coordinator training in San Diego, CA, 02/05/2007 - 02/08/2007
  - Acquisition of 22 laptops for Coordinators
  - Pending acquisition of retractable InfraGard banners for chapters
  - All 86 Chapters funded to foster priority program initiatives

- 2008 InfraGard Coordinator Training
  - Planning initiated with the Counterintelligence Division and Weapons of Mass Destruction Directorate for March 2008

- United States Public Private Partnership or USP3 (former DHS information sharing initiative)
  - The PPAU and Directorate of Intelligence are coordinating information sharing protocols with USP3's national governance

Intelligence Products

PROGRAM: Intelligence products (Intelligence Information Reports, Intelligence Bulletins, and Intelligence Assessments) sharing with InfraGard members. The PPAU considers the intelligence initiative its highest priority program.

BACKGROUND: In December 2004, the PPAU began providing intelligence community products to the InfraGard membership. Providing intelligence products was the result of close coordination with the Office of General Counsel and the Directorate of Intelligence (DI).

Concurrently, the PPAU requested that the InfraGard name be placed on the Intelligence Product Abstract, specifically the Dissemination Information section and the recipient list, which was accomplished. With InfraGard on the Abstract, the drafters or owners of intelligence products were made aware of InfraGard, educated as to what intelligence products could be shared with InfraGard based on the document's classification, and allowed the drafter or owner of an intelligence product to specifically check InfraGard as a desired recipient.

UPDATE: PPAU has established contacts with other FBI Headquarters Divisions to locate and obtain intelligence products for posting on the InfraGard Virtual Private Network (VPN). The current procedure for obtaining an intelligence product involves an SSA reviewing several Intelligence products daily. Products that appear appropriate for InfraGard are posted to the VPN, after the author of the Intelligence Product has granted permission. By posting intelligence products on the VPN two goals are achieved. The first goal was to increase participation in InfraGard through the VPN. The second goal was to educate the InfraGard members on what the FBI considered important. For instance, an InfraGard member can read an intelligence product and recognize a similar situation. In turn, the member could notify the local field office of the information so a case can be initiated and/or enhanced. During Fiscal Year (FY) 2005, 60 intelligence products were disseminated. For FY 2006, 145 intelligence products were disseminated. For the first half of FY 2007, 142 intelligence products have been disseminated. Average daily hits on the VPN have gone from 11,588 in January 2007 to 64,663 in June 2007.

Additionally, liaison continues with other intelligence community members, to obtain any and all unclassified intelligence to share with members. For instance, liaison has resulted in effective communication and/or information sharing with the Assistant Deputy Director of National Intelligence Open Source Center (ADDNI/OS), with the United States Public Private Partnership (USP3), state fusion centers, and with the Homeland Infrastructure Threat Risk Analysis Center (HITRAC).

Special Interest Groups

PROGRAM: Research and Technology Protection InfraGard Special Interest Group

BACKGROUND: The Research and Technology Protection (RTP) InfraGard Special Interest Group (SIG) is a collaborative effort of the Foreign-Counterintelligence and the Cyber Divisions of the FBI. It is intended to enhance the sharing of information among private sector stakeholders who, in partnership with the FBI, can assist in detecting, deterring, assessing, and preventing threats and attacks targeting the innovation that drives our national economy. It is the consortium of members representing U.S. firms, universities, national laboratories, sensitive government facilities and law enforcement with the common goal of protecting our country's research and technology.

UPDATE: The RTP-SIG was launched on September 25, 2006 and currently has 1,055 members 897 FBI Agents and 158 non-FBI .

PROGRAM: Chemical InfraGard Special Interest Group

BACKGROUND: The Chemical InfraGard Special Interest Group (SIG) is a collaborative effort of the Counterterrorism and the Cyber Divisions of the FBI. It is intended to enhance the sharing of information among private sector stakeholders who, in partnership with the FBI, can assist in detecting, deterring, assessing, and preventing threats and attacks targeting the innovation that drives our national economy. It is the consortium of members representing chemical security professionals, U.S. firms, and law enforcement with the common goal of protecting our country's chemical plants and industry.

UPDATE: The Chemical SIG was launched on December, 2005 and currently has 1,022 members 897 FBI Agents and 125 non-FBI.

PROGRAM: Food/Agriculture InfraGard Special Interest Group

BACKGROUND: The Food/Agriculture InfraGard Special Interest Group (SIG) is a collaborative effort of the Weapons of Mass Destruction Directorate and the Cyber Division of the FBI. It is intended to enhance information sharing among public and private sector stakeholders and subject matter experts who, in partnership with the FBI, can assist in detecting, deterring, assessing, and preventing threats and attacks targeting our nation's critical food supply economy. The Food/Ag SIG is a web-based consortium of InfraGard members affiliated with U.S. firms in the food and agriculture industry, state universities and research laboratories, and local, state and federal public sector organizations, including law enforcement agencies, all with the common goal of safeguarding our country's food supply.

UPDATE: The Food/Ag SIG was launched in February, 2006 and currently has1,030 members 897 FBI Agents and 133 non-FBI.

Co-sponsorship Agreements

PROGRAM: Co-sponsorship Agreement between the FBI, the Small Business Administration (SBA) and the Commerce Department's National Institutes of Standards and Technology (NIST), to furnish computer security for the small organization seminars.

BACKGROUND: Ninety-five percent of U.S. businesses, over 20 million, are small and medium-sized businesses (SMB) of 500 employees or less. A vulnerability common to a large percentage of all SMBs could pose a threat to the Nations's economic base. With information security, vulnerable SMBs run the risk of being compromised for use in crimes against governmental or large industrial systems. SMBs frequently cannot justify an extensive security program or a full-time expert. The Co-sponsorship Agreement seminars were developed by NIST to assist in filling a void; that is, to promote computer and information technology security with SMBs to safeguard their information systems. For its part, InfraGard's FBI and private sector members can use their public-private partnership to attend and advocate the seminars as they relate to critical infrastructure protection. The computer security for the small organization seminars are presented by NIST with the FBI and SBA contributing personnel and time to publicize and support the events. In June 2002, the initial Co-sponsorship Agreement was signed. The PPAU's role is to prepare an annual seminar schedule with the SBA and NIST; to establish liaison with local FBI Field Offices their InfraGard Chapter Coordinators for basic seminar support and to develop FBI speakers; to collaborate with the SBA on developing liaison between local FBI and SBA offices; and, to keep the InfraGard National Member Alliance informed. In January 2007, the Co-sponsorship Agreement was updated and signed by all parties.

UPDATE: For FY 2007, two seminars took place in January: Sacramento and San Jose. For the remainder of FY 2007, with InfraGard assistance, the following seminars are being planned: Boston, MA; Providence, RI; New Haven, CT; Philadelphia, PA; Birmingham and Mobile, AL; Chattanooga, Memphis and Nashville, TN; Atlanta and Savannah, GA; Tallahassee, Orlando and Miami, FL. Long Island, NY has been rescheduled to November 2007.